

日 本 国 特 許 庁
JAPAN PATENT OFFICE

19.2.2004

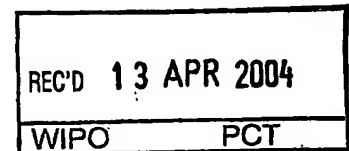
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2003年 2月21日

出 願 番 号
Application Number: 特願2003-045107
[ST. 10/C]: [JP2003-045107]

出 願 人
Applicant(s): 松下電器産業株式会社

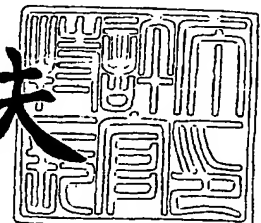


**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2004年 3月25日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 2022540519

【提出日】 平成15年 2月21日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 1/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 原田 俊治

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 中野 稔久

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003742

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理システム、記録媒体及び情報処理装置

【特許請求の範囲】

【請求項 1】 ソフトウェアを記録している記録媒体と、前記ソフトウェアを内部に記録し、前記ソフトウェアに従って動作する情報処理装置とから構成される情報処理システムであって、

前記記録媒体は、

ソフトウェアを記憶している通常記憶手段と、

前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、

耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段とを備え、

前記情報処理装置は、

前記ソフトウェアを記憶するための領域を備える記憶手段と、

前記記録媒体から前記許可指示を取得する取得手段と、

取得した前記許可指示に応じて、前記記録媒体から前記ソフトウェアを取得して前記記憶手段に書き込み、又は前記記憶手段に記憶されている前記ソフトウェアを非活性化する制御手段とを備える

ことを特徴とする情報処理システム。

【請求項 2】 ソフトウェアを記録している記録媒体であって、

ソフトウェアを記憶している通常記憶手段と、

前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、

耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアン

インストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段と
を備えることを特徴とする記録媒体。

【請求項 3】 前記通常記憶手段は、ソフトキーを用いて暗号化された暗号化ソフトウェアを記憶しており、

前記セキュア記憶手段は、前記ソフトキーを含む前記ライセンス情報を記憶しており、

前記耐タンパモジュール手段は、インストール可と判断する場合に、前記セキュア記憶領域に記憶されているライセンス情報からソフトキーを抽出し、抽出したソフトキーをセキュアに出力する

ことを特徴とする請求項 2 に記載の記録媒体。

【請求項 4】 前記セキュア記憶手段は、前記ソフトウェアの署名データを含む前記使用条件に係る前記ライセンス情報を記憶しており、

前記耐タンパモジュール手段は、インストールを可と判断する場合に、さらに、前記セキュア記憶手段に記憶されているライセンス情報から前記署名データを抽出し、抽出した前記署名データを出力する

ことを特徴とする請求項 2 に記載の記録媒体。

【請求項 5】 前記セキュア記憶手段は、前記使用条件が所定のキー情報を用いて暗号化されて生成された前記ライセンス情報を記憶しており、

前記耐タンパモジュール手段は、前記キー情報を記憶しており、前記キー情報を用いて、前記ライセンス情報を復号して前記使用条件を生成し、生成した使用条件に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断する

ことを特徴とする請求項 2 に記載の記録媒体。

【請求項 6】 前記セキュア記憶手段は、前記ライセンス情報の一部分を記憶しており、

前記耐タンパモジュール手段は、さらに、前記ソフトウェアの他の部分を記憶

しており、インストール又はアンインストールを可と判断する場合に、さらに、前記セキュア記憶手段に記憶されているライセンス情報の前記一部分を抽出し、抽出した前記一部分と記憶している前記他の部分とからライセンス情報を生成する

ことを特徴とする請求項 2 に記載の記録媒体。

【請求項 7】 前記セキュア記憶手段が記憶しているライセンス情報は、前記ソフトウェアの使用許可回数であり、

前記耐タンパモジュール手段は、前記使用許可回数が 0 より大きいと判断し、0 より大きいと判断する場合に、前記ソフトウェアの使用が許可されたとみなして、前記許可指示、前記ソフトキー、もしくは前記署名データのうち、少なくとも一つを出力し、さらに、前記使用許可回数から 1 減じて前記セキュア記憶手段に書き込む

ことを特徴とする請求項 2、請求項 3、請求項 4、請求項 5、又は請求項 6 に記載の記録媒体。

【請求項 8】 前記セキュア記憶手段が記憶しているライセンス情報は、前記ソフトウェアの使用許可回数であり、

前記耐タンパモジュール手段は、前記ソフトウェアのアンインストールが許可された場合に、前記許可指示を出力し、さらに、前記使用許可回数を 1 加算して前記セキュア記憶手段に書き込む

ことを特徴とする請求項 2、請求項 3、請求項 4、請求項 5、又は請求項 6 に記載の記録媒体。

【請求項 9】 ソフトウェアを記録している記録媒体から、前記ソフトウェアを取得して内部に記録し、前記ソフトウェアに従って動作する情報処理装置であって、

前記記録媒体は、

ソフトウェアを記憶している通常記憶手段と、

前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、

耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に

基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段とを備え、

前記情報処理装置は、

前記ソフトウェアを記憶するための領域を備える記憶手段と、

前記記録媒体から前記許可指示を取得する取得手段と、

取得した前記許可指示に応じて、前記記録媒体から前記ソフトウェアを取得して前記記憶手段に書き込み、又は前記記憶手段に記憶されている前記ソフトウェアを非活性化する制御手段と

を備えることを特徴とする情報処理装置。

【請求項 10】 前記セキュア記憶手段は、前記ソフトウェアの署名データを含む前記使用条件に係る前記ライセンス情報を記憶しており、

前記耐タンパモジュール手段は、インストールを可と判断する場合に、さらに、前記セキュア記憶手段に記憶されているライセンス情報から前記署名データを抽出し、抽出した前記署名データを出力し、

前記取得手段は、さらに、前記署名データを取得し、

前記制御手段は、取得した前記署名データ及び取得した前記ソフトウェアを用いて、取得した前記ソフトウェアの正当性の検証を行い、又は取得した前記署名データ及び前記記憶手段に記憶している前記ソフトウェアを用いて、前記ソフトウェアの正当性の検証を行い、検証が成功した場合に、取得した前記許可指示に応じて、取得した前記ソフトウェアを書き込み、又は記憶されている前記ソフトウェアを非活性化する

を備えることを特徴とする請求項 9 に記載の情報処理装置。

【請求項 11】 ソフトウェアを記録している記録媒体であって、

ソフトウェアを記憶している通常記憶手段と、

前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、

耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断し、許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出し、読み出した前記署名データを出力する耐タンパモジュール手段とを備えることを特徴とする記録媒体。

【請求項 12】 ソフトウェアを記録している記録媒体から前記ソフトウェアを読み出して内部に記憶する情報処理装置であって、

前記記録媒体は、ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断し、許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出し、読み出した前記署名データを出力する耐タンパモジュール手段とを備え、

前記情報処理装置は、

前記記録媒体から前記署名データ及び前記ソフトウェアを取得する取得手段と

、
取得した前記署名データを用いて、取得した前記ソフトウェアの検証を行い、検証が成功した場合に、取得した前記ソフトウェアを内部に記憶する記憶手段とを備えることを特徴とする情報処理装置。

【請求項 13】 ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備える記録媒体における前記耐タンパモジュール手段において用いられる制御方法であって、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断する判断ステップと、

可と判断する場合に、前記情報処理装置に対してインストール又はアンインス

トールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える書換ステップと

を含むことを特徴とする制御方法。

【請求項 14】 ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備える記録媒体における前記耐タンパモジュール手段において用いられる制御プログラムであって、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断する判断ステップと、

可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える書換ステップと

を含むことを特徴とする制御プログラム。

【請求項 15】 ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備える記録媒体における前記耐タンパモジュール手段において用いられる制御プログラムを記録しているコンピュータ読み取り可能なプログラム記録媒体であって、

前記制御プログラムは、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断する判断ステップと、

可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応

じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える書換ステップと

を含むことを特徴とする記録媒体。

【請求項 16】 ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備える記録媒体における前記耐タンパモジュール手段により用いられるインストール方法であって、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断する判断ステップと、

許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出す読出ステップと、

読み出した前記署名データを出力する出力ステップと

を含むことを特徴とするインストール方法。

【請求項 17】 ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備える記録媒体における前記耐タンパモジュール手段により用いられるインストールプログラムであって、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断する判断ステップと、

許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出す読出ステップと、

読み出した前記署名データを出力する出力ステップと

を含むことを特徴とするインストールプログラム。

【請求項 18】 ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備えるソフトウェア記録媒体における前記耐タ

ンパモジュール手段により用いられるインストールプログラムを記録しているコンピュータ読み取り可能なプログラム記録媒体であって、

前記インストールプログラムは、

前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断する判断ステップと、

許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出す読出ステップと、

読み出した前記署名データを出力する出力ステップと
を含むことを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンピュータソフトウェアのライセンス管理技術に関する。

【0002】

【従来の技術】

従来よりコンピュータプログラムのライセンスを管理する様々な技術が提案されている。

特許文献1は、記録媒体に記録されているアプリケーションプログラムが無制限にインストールされることを防止し、不正な使用を解消することを目的として、インストール実行に応じてインストール回数を記録媒体の記録再生領域に記録しておき、アプリケーションプログラムを他の記録媒体へインストールする要求があった場合に、記録されている過去のインストール回数を確認し、そのインストール回数が所定回数未満であったときのみ、インストールを実行するインストール制御技術を開示している。

【0003】

【特許文献1】

特開平10-27426号公報

また、特許文献2は、ICカードに格納された情報に基づいて、ソフトウェアの不正使用を防止するソフトウェアライセンス管理システムを開示している。前

記管理システムは、ソフトウェア記録媒体と、該ソフトウェアのライセンス管理情報を格納したICカードと、カードリーダライタを接続した情報処理端末機とを具備しており、前記管理システムは、ソフトウェア購入者が個々に保持する前記情報処理端末機のカードリーダライタを介して前記ICカードからライセンス管理情報を読み出す手段と、該ライセンス管理情報に基づいてインストールまたはアンインストールする手段からなり、前記ICカードにインストールした情報処理端末機を特定する情報を記録する。

【0004】

【特許文献2】

特開 2002-268764号公報

さらに、特許文献3は、ソフトウェアのライセンス不正利用を抑止することを目的とするソフトウェアコピーガード実現方法を開示している。前記コピーガード実現方法は、揮発性記憶領域と不揮発性記憶領域が内蔵されたカートリッジに着脱可能な記録媒体が挿入され、カートリッジ内の不揮発性記憶領域に格納された認証アルゴリズムと、ソフトウェアのインストールプログラムと、ソフトウェアをインストールするシステム装置固有のシステム情報と、記録媒体が持つソフトウェア固有の情報と、カートリッジアクセス装置とを利用する。カートリッジは、記録媒体が持つソフトウェア固有の情報及び端末装置に固有の端末固有情報を用いて、認証データを生成して内部に記録し、認証データに基づいてソフトウェアの端末装置へのインストールの可否を判断する。

【0005】

【特許文献3】

特開 2002-182769号公報

【0006】

【発明が解決しようとする課題】

しかしながら、第1に、特許文献1により開示されているインストール制御技術によると、記録媒体に記録されているインストール回数によりインストールを実行するか否かを判断するので、無制限にアプリケーションプログラムがインストールされることを防止できるものの、悪意のある第三者が、記録媒体の記録再

生領域に記録されているインストール回数を改竄すれば、無制限にアプリケーションプログラムをインストールすることができるという問題点（課題1）がある。

【0007】

また、前記インストール制御技術によると、前記記録媒体からインストール回数が、前記記録媒体とインストールの対象となる端末装置との間の通信路上を流れることにより、端末装置に伝達され、端末装置においてインストール回数を受け取り、受け取ったインストール回数を用いて、端末装置が、インストールの可否を判定する。ここで、悪意のある第三者が、前記通信路上において、インストール回数を改竄すれば、上記と同様に、無制限にアプリケーションプログラムをインストールすることができるという問題点（課題2）がある。

【0008】

さらに、前記インストール制御技術によると、記録媒体上においてアプリケーションプログラムとインストール回数とが対応付けて記録されているので、悪意のある第三者が、記録媒体上におけるアプリケーションプログラムとインストール回数との対応付けを不正に改竄すれば、例えば、安価なプログラムを正規に購入し、購入した安価なプログラムとインストール回数との対応付けを、正規に購入していない高価なプログラムと前記インストール回数との対応付けに変更すれば、前記高価なプログラムを、インストールすることができるという問題点（課題3）がある。

【0009】

第2に、特許文献2により開示された管理システムによると、該ソフトウェアのライセンス管理情報がICカードに格納されているので、悪意のある第三者によっても、ICカードに格納されているライセンス管理情報の改竄は容易ではない。従って課題1に指摘するような問題点が発生する可能性は低い。

また、前記管理システムによると、前記ICカードからライセンス管理情報が、前記ICカードとインストールの対象となる情報処理端末機との間の通信路上を流れることにより、情報処理端末機に伝達され、情報処理端末機においてライセンス管理情報を受け取り、受け取ったライセンス管理情報を用いて、情報処理

端末機が、インストールの可否を判定する。ここで、悪意のある第三者が、前記通信路上において、ライセンス管理情報を改竄すれば、特許文献1により開示されているインストール制御技術による場合と同様に、無制限にアプリケーションプログラムをインストールすることができるという問題点（課題2）がある。

【0010】

さらに、前記管理システムによると、ソフトウェア記録媒体とICカードとが対応付けられているので、悪意のある第三者が、例えば、安価なソフトウェアが記録されている第1のソフトウェア記録媒体及び100台分のライセンス管理情報を記録した第1のICカードと、高価なソフトウェアが記録されている第2のソフトウェア記録媒体及び1台分のライセンス管理情報を記録した第2のICカードとを正規に購入し、第2のソフトウェア記録媒体が第1のICカードに対応付くように、第2のソフトウェア記録媒体を改竄すれば、前記高価なソフトウェアを、インストールすることができるという問題点（課題3）がある。

【0011】

第3に、特許文献3により開示されたコピーガード実現方法によると、ソフトウェアのインストールの可否を判断するために用いられる認証データがカートリッジ内に記録されているので、悪意のある第三者によっても、カートリッジに記録されている認証データの改竄は容易ではない。従って課題1に指摘するような問題点が発生する可能性は低い。

【0012】

また、前記コピーガード実現方法によると、悪意のある第三者が、カートリッジアクセス装置とカートリッジの間の通信路上を流れるライセンス関連情報を改竄すれば、特許文献1により開示されているインストール制御技術による場合と同様に、無制限にアプリケーションプログラムをインストールすることができるという問題点（課題2）がある。

【0013】

さらに、前記コピーガード実現方法によると、悪意のある第三者が、記録媒体とカートリッジとの対応付けを改竄すれば、特許文献2により開示された管理システムの場合と同様に、例えば、正規に購入していない高価なソフトウェアを、

インストールすることができるという問題点（課題 3）がある。

本発明は、上記の問題点（課題 1～3）を解決し、コンピュータソフトウェアが記録されている記録媒体上の改竄がされにくく、ソフトウェアがインストールされる対象となる端末装置と前記記録媒体との間の通信路における不当な攻撃を避けることができ、またソフトウェアとライセンス情報との対応関係を不正に更新することができない情報処理システム、記録媒体、情報処理装置、制御方法、制御プログラム、インストール方法、インストールプログラム及び記録媒体を提供することを目的とする。

【0014】

【課題を解決するための手段】

上記目的を達成するために、本発明は、コンピュータソフトウェアを記録している記録媒体である。前記記録媒体は、セキュア記憶領域及び通常記憶領域を含む情報記憶部と、耐タンパモジュール部とを備えている。

通常記憶領域には、コンピュータ命令の実行手順を示すコンピュータソフトウェアが記憶されており、セキュア記憶領域には、前記コンピュータソフトウェアの使用許可数を示すライセンス数と、前記コンピュータソフトウェアの署名データとが対応付けて記録されている。

【0015】

耐タンパモジュール部は、前記コンピュータソフトウェアのインストール対象となる端末装置との間で、相互に機器認証を行い、相手が正当な装置であることを確認する。

相手が正当な装置があると確認された場合に、耐タンパモジュール部は、端末装置から暗号化端末固有情報を取得する。暗号化端末固有情報は、端末固有情報が暗号化されたものであり、端末固有情報は、前記端末装置に固有の情報である。耐タンパモジュール部は、取得した暗号化端末固有情報を復号して端末固有情報を得、得られた端末固有情報がセキュア記憶領域にすでに記憶されているなら、ソフトウェアの再インストールとみなす。記憶されていないなら、新規インストールとみなし、前記端末固有情報をセキュア記憶領域に書き込む。耐タンパモジュール部は、セキュア記憶領域に記憶されているライセンス数をチェックし、

ライセンス数が所定数以内であれば、コンピュータソフトウェアとコンピュータソフトウェアの署名データとを端末装置へ出力する。

【0016】

端末装置は、コンピュータソフトウェアと署名データとを受け取り、受け取った署名データを検証し、検証が成功すれば、受け取ったコンピュータソフトウェアを内部にインストールする。

一方、耐タンパモジュール部は、ライセンス数を1だけ減じるように更新する。

【0017】

【発明の実施の形態】

1. 実施の形態1

本発明に係る1個の実施の形態としてのソフトウェア管理システム10について説明する。

1. 1 ソフトウェア管理システム10の構成

ソフトウェア管理システム10は、図1に示すように、ソフトウェア書込装置100、可搬型のメモリカード200及び情報処理装置300から構成されている。

【0018】

ソフトウェア書込装置100は、ソフトウェア提供者が有しているパーソナルコンピュータ等により構成されるコンピュータシステムであり、ソフトウェア販売店や、CE（コンシューマエレクトロニクス）機器メーカーの顧客サービスセンターにおいて利用される。ソフトウェア書込装置100は、コンピュータにより実行されるアプリケーションプログラム、前記アプリケーションプログラムの不具合などを修正するためのバグ修正プログラム、前記アプリケーションプログラムの新機能追加のためのバージョンアッププログラムなどのソフトウェアをメモリカード200に書き込む。前記ソフトウェアは、複数のコンピュータ命令から構成され、これらのコンピュータ命令の実行手順を示すものである。前記ソフトウェアの書き込まれたメモリカード200は、利用者に有償又は無償で提供される。

【0019】

情報処理装置 300 は、利用者が有しているパーソナルコンピュータや家庭電化製品などの CE 機器である。利用者により前記ソフトウェアが書き込まれたメモリカード 200 が情報処理装置 300 に挿入される。情報処理装置 300 は、メモリカード 200 に書き込まれているソフトウェアを読み出して、内部に記憶、つまりインストールする。情報処理装置 300 は、内部に記憶しているソフトウェアに従って動作する。このようにして、利用者は、そのソフトウェアを利用することができる。

【0020】

また、情報処理装置 300 は、内部に記憶しているソフトウェアをアンインストールする。こうして、利用者のそのソフトウェアを非活性化することができる。

1. 2 ソフトウェア書込装置 100 の構成

ソフトウェア書込装置 100 は、図 2 に示すように、認証部 111、暗号化部 112、情報記憶部 113、制御部 114 及び暗号化部 118 から構成されている。また、ソフトウェア書込装置 100 には、入力部 115 及び表示部 116 が接続されている。

【0021】

ソフトウェア書込装置 100 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。また、入力部 115 は、具体的には、キーボードであり、表示部 116 は、ディスプレイユニットである。前記 RAM 又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、ソフトウェア書込装置 100 は、その機能を達成する。

【0022】

なお、図 2 において、各ブロックは、接続線により他のブロックと接続されている。ただし、一部の接続線を省略している。ここで、各接続線は、信号や情報が伝達される経路を示している。また、暗号化部 112 を示すブロックに接続し

ている複数の接続線のうち、接続線上に鍵マークが付されているものは、暗号化部 112 へ鍵としての情報が伝達される経路を示している。また、他の図面についても同様である。

【0023】

(1) 情報記憶部 113

情報記憶部 113 は、図 2 に示すように、ソフトウェア管理テーブル 121、ソフトウェア 122、ソフトウェア 123、・・・をセキュアに記憶している。

ソフトウェア管理テーブル 121 は、ソフト ID、ソフトキー及びインストール回数情報から構成されるソフトウェア管理情報を複数個含むデータテーブルである。

【0024】

ソフト ID は、当該ソフトウェアを識別するための識別番号であり、64 ビット長である。

ソフトキーは、当該ソフトウェアを暗号化する際に用いられる暗号鍵であり、56 ビット長である。

インストール回数情報は、16 ビット長であり、当該ソフトウェアに割り当てられたインストール許可回数である。例えば、インストール回数情報が「10」である場合に、利用者に対して、当該ソフトウェアを最大 10 回までインストールすることが許可される。また、インストール回数情報として「FFFF」（16 進数）が指定された場合には、無制限にインストールが可能であることを示すものとする。ここでは、インストール回数情報は、固定値をとっているが、利用者の購入数に応じて可変であるように設定してもよい。

【0025】

ソフトウェア 122、ソフトウェア 123、・・・は、それぞれ、コンピュータプログラムであり、ソフト ID により識別される。

(2) 入力部 115

入力部 115 は、ソフトウェア書込装置 100 の操作者からソフトウェアの指定を受け付け、指定を受け付けたソフトウェアを識別するソフト ID を情報記憶部 113 から取得し、取得したソフト ID を制御部 114 へ出力する。

【0026】

(3) 認証部 111

メモリカード 200 が操作者によりソフトウェア書込装置 100 に挿入されると、認証部 111 は、メモリカード 200 が有する認証部 211 との間で、チャレンジレスポンス型の相互の機器認証を行う。

具体的には、認証部 111 は、認証部 211 を認証する。次に、認証部 111 は、認証部 211 により、認証を受ける。

【0027】

認証部 111 及び認証部 211 の認証が共に成功した場合に、認証部 111 と認証部 211 との間での上記チャレンジレスポンス型の認証のプロセスにおいて使用される乱数情報に基づいて、相互の認証の都度異なる 64 ビット長のセッション鍵を生成し、生成したセッション鍵を認証部 211 との間で秘密に共有する。次に認証部 111 は、生成したセッション鍵を暗号化部 118 へ出力する。

【0028】

認証部 111 は、両者の認証が成功した場合に、認証の成功を示す認証成功情報を制御部 114 へ出力し、認証が失敗した場合に、認証の失敗を示す認証失敗情報を制御部 114 へ出力する。

なお、チャレンジレスポンス型の機器認証については、公知であるので、説明を省略する。

【0029】

(4) 制御部 114

制御部 114 は、入力部 115 からソフト ID を受け取る。また、制御部 114 は、認証部 111 から認証成功情報又は認証失敗情報を受け取る。

認証部 111 から認証成功情報を受け取ると、制御部 114 は、暗号化部 118 に対して受け取ったソフト ID を出力し、また暗号化部 118 に対してソフトウェア管理情報を暗号化してメモリカード 200 へ書き込む旨の暗号化指示を出力する。また、制御部 114 は、暗号化部 112 に対して受け取ったソフト ID を出力し、暗号化部 112 に対してソフトウェアを暗号化してメモリカード 200 へ書き込む旨の暗号化指示を出力する。

【0030】**(5) 暗号化部 118**

暗号化部 118 は、制御部 114 からソフト ID 及び暗号化指示を受け取る。
また、暗号化部 118 は、認証部 111 からセッション鍵を受け取る。

制御部 114 からソフト ID 及び暗号化指示を受け取ると、暗号化部 118 は、ソフトウェア管理テーブル 121 から、前記ソフト ID を含むソフトウェア管理情報を読み出し、認証部 111 から受け取ったセッション鍵を用いて、読み出したソフトウェア管理情報に暗号化アルゴリズム E3 を施し、暗号化ソフトウェア管理情報を生成する。次に、暗号化部 118 は、生成した暗号化ソフトウェア管理情報をメモ리카ード 200 へ出力する。

【0031】**(6) 暗号化部 112**

暗号化部 112 は、制御部 114 からソフト ID 及び暗号化指示を受け取る。

制御部 114 からソフト ID 及び暗号化指示を受け取ると、ソフトウェア管理テーブル 121 から前記ソフト ID を含むソフトウェア管理情報を読み出し、読み出したソフトウェア管理情報からソフトキーを抽出する。次に、暗号化部 112 は、情報記憶部 113 から受け取ったソフト ID により識別されるソフトウェアを読み出し、抽出したソフトキーを鍵として用いて、読み出したソフトウェアに暗号化アルゴリズム E1 を施し、暗号化ソフトウェアを生成する。

【0032】

ここで、暗号化アルゴリズム E1 は、DES (Data Encryption Standard) により規定されたものである。

なお、ソフトキーのビット長、暗号化アルゴリズムについては、上記に説明したものに限定されない。

次に、暗号化部 112 は、生成した暗号化ソフトウェアをメモ리카ード 200 へ出力する。

【0033】**(7) 表示部 116**

表示部 116 は、制御部 114 の制御により各種情報を表示する。

1. 3 メモリカード 200 の構成

メモリカード 200 は、図 2 及び図 3 に示すように、特別に許可された経路を除いて、外部から読み書きできない耐タンパモジュール部 210 及び情報記憶部 220 から構成されている。耐タンパモジュール部 210 は、認証部 211、復号部 212、暗号化部 213 及び判定部 214 から構成され、情報記憶部 220 は、第 1 記憶領域 221 及び第 2 記憶領域 222 から構成されている。

【0034】

ここで、耐タンパモジュール部 210 は、具体的には、耐タンパ性を有する耐タンパハードウェアにより構成されている。なお、耐タンパモジュール部 210 は、耐タンパソフトウェア、又は耐タンパハードウェア及び耐タンパソフトウェアの組み合わせから構成されているとしてもよい。

また、耐タンパモジュール部 210 は、具体的には、マイクロプロセッサ、及び ROM、RAM などのメモリ部から構成され、前記メモリ部には、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、耐タンパモジュール部 210 は、その機能を達成する。

【0035】

情報記憶部 220 は、具体的には、大容量のフラッシュメモリにより構成されている。

(1) 第 1 記憶領域 221

第 1 記憶領域 221 は、特別の許可がなくとも、外部からアクセスすることが許されている領域である。

【0036】

第 1 記憶領域 221 は、1 個以上の暗号化ソフトウェアを記憶するための領域を備えている。

(2) 第 2 記憶領域 222

第 2 記憶領域 222 は、ソフトウェア管理情報テーブル 231 を有している。

ソフトウェア管理情報テーブル 231 は、図 4 に示すように、複数個のソフトウェア管理情報 241、242、・・・を記憶するための領域を含んでいる。

【0037】

ソフトウェア管理情報241は、この図に示すように、ソフトID、ソフトキー、インストール回数情報及び複数の装置IDを含む。ソフトID、ソフトキー及びインストール回数情報については、上述した通りであるので説明を省略する。

装置IDは、ソフトウェアがインストールされる対象となる情報処理装置を一意に識別するための識別番号である。

【0038】

なお、図4に示すソフトウェア管理情報241において、括弧内に表示されている文字列「SID1」、「XYZ123」、「10」、「#1」及び「#2」は、それぞれ、ソフトID、ソフトキー、インストール回数情報及び2個の装置IDの具体例としての値である。

なお、図4に示すソフトウェア管理情報241は、複数の装置IDを含むように示されているが、ソフトウェア書込装置100からメモリカード200に、ソフトウェア管理情報が書き込まれる時点においては、まだ、ソフトウェア管理情報241は、複数の装置IDを含んでいない。装置IDは、ソフトウェアが情報処理装置にインストールされたときに、ソフトウェア管理情報241内に書き込まれる。利用者は、提供されたメモリカードを用いて、初めてソフトウェアをインストールする際には、任意の情報処理装置に、ソフトウェアのインストールを実行することができる。

【0039】

ソフトウェア管理情報242、・・・については、ソフトウェア管理情報241と同様であるので、説明を省略する。

(3) 認証部211

メモリカード200がソフトウェア書込装置100に挿入されると、認証部211は、ソフトウェア書込装置100が有する認証部111との間で、チャレンジレスポンス型の相互の機器認証を行う。

【0040】

具体的には、認証部211は、認証部111により認証を受ける。次に、認証

部 2 1 1 は、認証部 1 1 1 の認証を行う。

認証部 2 1 1 は、両者の認証が成功した場合に、認証部 1 1 1 との間で上記チャレンジレスポンス型の認証のプロセスにおいて使用される乱数情報に基づいて、相互認証の都度、異なるセッション鍵を生成し、認証部 2 1 1 は、生成したセッション鍵を復号部 2 1 2 へ出力し、さらに認証の成功を示す第 1 認証成功情報を判定部 2 1 4 へ出力する。一方、認証が失敗した場合に、認証部 2 1 1 は、認証の失敗を示す第 1 認証失敗情報を判定部 2 1 4 へ出力する。

【0041】

また、認証部 2 1 1 は、情報処理装置 3 0 0 が有する認証部 3 1 1 との間で、チャレンジレスポンス型の相互の認証を行う。具体的には、認証部 2 1 1 は、認証部 3 1 1 により認証を受ける。次に、認証部 2 1 1 は、認証部 3 1 1 の認証を行う。

両者の認証が成功した場合に、認証部 2 1 1 は、認証部 3 1 1 との間で上記チャレンジレスポンス型の認証のプロセスにおいて使用される乱数情報に基づいて、相互の認証の都度、異なるセッション鍵を生成し、認証部 3 1 1 との間で生成したセッション鍵を秘密に共有する。認証部 2 1 1 は、生成したセッション鍵を復号部 2 1 2 及び暗号化部 2 1 3 へ出力し、さらに、認証の成功を示す第 2 認証成功情報を判定部 2 1 4 へ出力する。

【0042】

認証が失敗した場合に認証部 2 1 1 は、認証の失敗を示す第 2 認証失敗情報を判定部 2 1 4 へ出力する。メモリカード 2 0 0 より以降の処理は中止される。従って、この場合、情報処理装置 3 0 0 に、メモリカード 2 0 0 からソフトウェアがインストールされることはない。インストール処理が中止されたことは、メモリカード 2 0 0 から情報処理装置 3 0 0 に通知され、情報処理装置 3 0 0 の利用者に知らされる。

【0043】

なお、相互の機器認証のプロセスにおけるセッション鍵の共有方法については、公知であるので、説明を省略する。

(4) 復号部 2 1 2

復号部 212 は、認証部 211 からセッション鍵を受け取る。

また、復号部 212 は、ソフトウェア書込装置 100 から暗号化ソフトウェア管理情報を受け取り、受け取ったセッション鍵を用いて受け取った暗号化ソフトウェア管理情報に復号アルゴリズム D3 を施してソフトウェア管理情報を生成し、生成したソフトウェア管理情報を判定部 214 へ出力する。

【0044】

さらに、復号部 212 は、情報処理装置 300 の暗号化部 312 から、暗号化区分、暗号化ソフト ID 及び暗号化装置 ID を受け取り、受け取ったセッション鍵を用いて、受け取った暗号化区分、暗号化ソフト ID 及び暗号化装置 ID に、復号アルゴリズム D3 を施して、それぞれ、区分、ソフト ID 及び装置 ID を生成し、生成した区分、ソフト ID 及び装置 ID を判定部 214 へ出力する。

【0045】

ここで、復号アルゴリズム D3 は、暗号化アルゴリズム E3 に対応するものであり、暗号化アルゴリズム E3 を用いて生成された暗号文を、復号するために用いられる。

また、アンインストールの際に、復号部 212 は、暗号化部 312 から暗号化完了情報を受け取り、認証部 211 から受け取ったセッション鍵を用いて、受け取った暗号化完了情報に復号アルゴリズム D3 を施して、完了情報及び乱数 R' を生成し、生成した完了情報及び乱数 R' を判定部 214 へ出力する。

【0046】

(5) 暗号化部 213

暗号化部 213 は、認証部 211 からセッション鍵を受け取る。また、暗号化部 213 は、判定部 214 より、ソフトキーを受け取る。次に、暗号化部 213 は、受け取ったセッション鍵を用いて、受け取ったソフトキーに暗号化アルゴリズム E4 を施して、暗号化ソフトキーを生成する。

【0047】

ここで、暗号化アルゴリズム E4 は、DES により規定されたものである。

次に、暗号化部 213 は、生成した暗号化ソフトキーを情報処理装置 300 へ出力する。

また、アンインストールの際には、暗号化部 213 は、判定部 214 から、乱数 R 及びアンインストール可否情報を受け取り、認証部 211 から受け取ったセッション鍵を用いて、受け取った乱数 R 及びアンインストール可否情報に暗号化アルゴリズム E4 を施して、暗号化アンインストール可否情報を生成し、生成した暗号化アンインストール可否情報を情報処理装置 300 へ出力する。

【0048】

(6) 判定部 214

判定部 214 は、認証部 211 から第 1 認証成功情報又は第 1 認証失敗情報を受け取り、また認証部 211 から第 2 認証成功情報又は第 2 認証失敗情報を受け取る。

(A) 第 1 認証成功情報を受け取った場合に、判定部 214 は、さらに復号部 212 からソフトウェア管理情報を受け取り、受け取ったソフトウェア管理情報をソフトウェア管理情報テーブル 231 内に追加して書き込む。

【0049】

(B) また、第 2 認証成功情報を受け取った場合に、判定部 214 は、さらに、復号部 212 から区分、ソフト ID 及び装置 ID を受け取る。

次に、判定部 214 は、受け取った区分がインストールを示すか又はアンインストールを示すかを判断する。

(B1) インストールを示す場合

受け取った区分がインストールを示すと判断する場合に、判定部 214 は、次に、受け取ったソフト ID を含むソフトウェア管理情報をソフトウェア管理情報テーブル 231 から抽出し、抽出したソフトウェア管理情報に、受け取った装置 ID が含まれているか否かを判断する。

【0050】

(a1) 装置 ID が含まれていないと判断する場合には、判定部 214 は、新しい情報処理装置へのインストールの要請であると判断し、次に、前記ソフトウェア管理情報に含まれるインストール回数情報をチェックする。

このとき、(a1-1) インストール回数情報が 1 以上であれば、判定部 214 は、インストールを許可すると判定し、前記復号部 212 より受取った装置 I

Dを前記ソフトウェア管理情報に追加して書き込み、前記ソフトウェア管理情報に含まれるインストール回数情報から1を減算して得られる値を、新たにインストール回数情報として、ソフトウェア管理情報テーブル231内の前記ソフトウェア管理情報内に上書きする。さらに、判定部214は、前記ソフトウェア管理情報に含まれるソフトキーを暗号化部213に出力する。

【0051】

一方、(a1-2)前記インストール回数情報のチェックにおいて、インストール回数情報が零であれば、判定部214は、インストールを許可しないと判定し、以降の処理を中止する。従って、この場合、情報処理装置300に、メモリカード200からソフトウェアがインストールされることはない。インストール処理が中止されたことは、メモリカード200から情報処理装置300に通知され、情報処理装置300は、この旨を表示することにより、利用者に通知する。

【0052】

(a2)装置IDが含まれていると判断する場合には、判定部214は、既にインストール済みの情報処理装置への再インストールの要請であると判断し、前記ソフトウェア管理情報に含まれるソフトキーを暗号化部213に出力する。

(B2) アンインストールを示す場合

受け取った区分がアンインストールを示すと判断する場合に、判定部214は、さらに、受け取ったソフトIDを含むソフトウェア管理情報をソフトウェア管理情報テーブル231から抽出し、抽出したソフトウェア管理情報に、復号部212から受け取った装置IDが含まれているか否か判断する。

【0053】

ここで、装置IDが含まれないと判断する場合に、判定部214は、アンインストール不可と判定してアンインストール不可を示す8ビット長のアンインストール可否情報を生成する。

一方、装置IDが含まれると判断する場合は、判定部214は、アンインストール可と判定してアンインストール可を示す8ビット長のアンインストール可否情報を生成する。

【0054】

次に、判定部 214 は、56 ビット長の乱数 R を生成し、生成した乱数 R を保持する。次に、判定部 214 は、生成した乱数 R 及びアンインストールの可否を示すアンインストール可否情報を暗号化部 213 へ出力する。

また、判定部 214 は、完了情報及び乱数 R' を受け取り、受け取った乱数 R' と保持している乱数 R とが一致するか否かを判断する。ここで、一致しない場合には、アンインストール処理を中止する。一方、一致する場合には、判定部 214 は、さらに、完了情報がアンインストールが完了したことを示しているか否かを判断し、完了情報がアンインストールが完了したことを示していない場合は、以降のアンインストール処理を中止する。

【0055】

ここで、完了情報がアンインストールが完了したことを示している場合は、判定部 214 は、ソフトウェア管理情報に含まれるインストール回数情報に「1」の値を加算し、得られた値を、新たにインストール回数情報として、ソフトウェア管理テーブル 231 内の前記ソフトウェア管理情報内に上書きする。

(C) 第 1 認証失敗情報又は第 2 認証失敗情報を受け取った場合に、判定部 214 は、以降の処理を中止する。

【0056】

なお、実施の形態 1 では、判定部 214 は、まずソフトウェア管理テーブルに装置 ID が含まれているか否かをチェックし、次に、インストール回数情報のチェックを行うとしているが、これに限定されるものではない。まずインストール回数情報のチェックを行い、次に装置 ID のチェックを行うように構成しても良い。

【0057】

1. 4 情報処理装置 300 の構成

情報処理装置 300 は、図 3 に示すように、インストール処理部 310、ソフトウェア格納部 320、制御部 321、表示部 322、入力部 323、ソフトウェア実行部 324 及び復号部 325 から構成されている。インストール処理部 310 は、さらに、認証部 311、暗号化部 312、復号部 313、復号部 314、暗号化部 315、装置 ID 格納部 316、装置固有鍵生成部 317、ソフト I

D取得部318及び乱数格納部326から構成されている。

【0058】

情報処理装置300は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどのメモリ部、キーボード、マウスなどの入力部、ディスプレイユニットなどの表示部から構成されるコンピュータシステムである。前記メモリ部には、インストール処理用のコンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記インストール処理用のコンピュータプログラムに従って動作することにより、情報処理装置300は、インストール処理の機能を達成する。また、メモリカードから、ソフトウェアがインストールされた暁には、前記マイクロプロセッサが、前記インストールされたソフトウェアに従って動作することにより、情報処理装置は、インストールされたソフトウェアが提供する機能を達成する。

【0059】

(1) ソフトウェア格納部320

ソフトウェア格納部320は、具体的には、ハードディスクユニットから構成され、メモリカード200からインストールされる暗号化ソフトウェアを1個以上記憶する領域を備えている。

(2) 装置ID格納部316

装置ID格納部316は、情報処理装置300に固有の装置IDを、書き換え不可能な形で記憶している。装置IDは、64ビット長のデータであり、情報処理装置300を一意に識別する識別情報である。

【0060】

(3) ソフトID取得部318

ソフトID取得部318は、利用者がインストールを指定したソフトウェアのソフトIDを取得する。

ソフトIDの取得の具体的な方法としては、例えば、利用者により情報処理装置300にメモリカード200が装着された際に、情報処理装置300が有する表示部322は、メモリカード200内に記憶されている暗号化ソフトウェアの一覧を表示する。入力部323は、その一覧からインストールしたいソフトウエ

アの指定を利用者のマウスの操作により、受け付ける。その結果として、ソフト I D 取得部 318 は、指定を受け付けたソフトウェアに対応するソフト I D を取得する。

【0061】

(4) 認証部 311

メモリカード 200 が利用者により情報処理装置 300 に挿入されると、認証部 311 は、メモリカード 200 が有する認証部 211 との間で、チャレンジレスポンス型の相互の機器認証を行う。具体的には、認証部 311 は、認証部 211 を認証する。次に、認証部 311 は、認証部 211 により、認証を受ける。両方の装置の認証が成功した場合にのみ、相互の認証が成功したものと見做される。

【0062】

両者の認証が成功した場合に、認証部 311 及び認証部 211 との間での上記チャレンジレスポンス型の認証のプロセスにおいて使用される乱数情報に基づいて、相互の認証の都度、異なるセッション鍵を生成し、生成したセッション鍵を認証部 211 との間で秘密に共有する。

次に、認証部 311 は、生成したセッション鍵を暗号化部 312 及び復号部 313 へ出力する。

【0063】

認証に失敗した場合に、認証部 311 は、以降の処理を中止する。従って、この場合に、情報処理装置 300 が、メモリカード 200 からソフトウェアを読み出すことはない。なお、チャレンジレスポンス型の認証、及びセッション鍵の共有方法については、公知であるので、説明を省略する。

(5) 暗号化部 312

暗号化部 312 は、認証部 311 からセッション鍵を受け取る。

【0064】

次に、暗号化部 312 は、制御部 321 からソフトウェアのインストール又はアンインストールを示す区分を受け取り、ソフト I D 取得部 318 からソフト I D を受け取り、装置 I D 格納部 316 から装置 I D を読み出し、認証部 311 よ

り受け取ったセッション鍵を用いて、前記区分、前記ソフトID及び前記装置IDに暗号化アルゴリズムE3をそれぞれ施して暗号化区分、暗号化ソフトID及び暗号化装置IDを生成する。

【0065】

ここで、暗号化アルゴリズムE3は、DESにより規定されたものである。

次に、暗号化部312は、生成した暗号化区分、暗号化ソフトID及び暗号化装置IDをメモ리카ード200へ出力する。

また、アンインストールの際に、暗号化部312は、完了情報及び乱数R'を受け取り、認証部311から受け取ったセッション鍵を用いて、受け取った完了情報及び乱数R'に暗号化アルゴリズムE3を施して、暗号化完了情報を生成し、生成した暗号化完了情報を、復号部212へ出力する。

【0066】

(6) 復号部313

復号部313は、認証部311からセッション鍵を受け取る。

次に、復号部313は、メモ리카ード200から、暗号化ソフトキーを受け取り、受け取ったセッション鍵を用いて、受け取った暗号化ソフトキーに復号アルゴリズムD4を施して、ソフトキーを生成する。

【0067】

ここで、復号アルゴリズムD4は、DESにより規定されたものであり、暗号化アルゴリズムE4に対応するものである。復号アルゴリズムD4は、暗号化アルゴリズムE4を用いて生成された暗号文を復号する。

次に、復号部313は、生成したソフトキーを復号部314へ出力する。

また、アンインストールの際には、復号部313は、メモ리카ード200から暗号化アンインストール可否情報を受け取り、認証部311から受け取ったセッション鍵を用いて、受け取った暗号化アンインストール可否情報に復号アルゴリズムD4を施して、アンインストール可否情報及び乱数R'を生成し、生成したアンインストール可否情報及び乱数R'を制御部321へ出力する。

【0068】

(7) 復号部314

復号部 314 は、メモリカード 200 から、前記ソフト ID に対応する暗号化ソフトウェアを受け取る。また、復号部 313 からソフトキーを受け取る。

次に、復号部 314 は、受け取ったソフトキーを用いて、受け取った暗号化ソフトウェアに復号アルゴリズム D1 を施して、ソフトウェアを生成する。

【0069】

ここで、復号アルゴリズム D1 は、DES により規定されたものであり、暗号化アルゴリズム E1 に対応するものである。復号アルゴリズム D1 は、暗号化アルゴリズム E1 を用いて生成された暗号文を復号する。

次に、復号部 314 は、生成したソフトウェアを暗号化部 315 へ出力する。

(8) 乱数格納部 326

乱数格納部 326 は、64 ビット長の乱数を格納している。

【0070】

(9) 装置固有鍵生成部 317

装置固有鍵生成部 317 は、装置 ID 格納部 316 から、装置 ID を読み出し、次に、乱数格納部 326 から 64 ビット長の乱数を読み出し、読み出した乱数をキーとして、読み出した装置 ID に暗号化アルゴリズム F を施して、装置 ID に対応する装置固有鍵を秘密に生成し、生成した装置固有鍵を暗号化部 315 及び復号部 325 へ出力する。

【0071】

ここで暗号化アルゴリズム F は DES により規定されたものである。なお、乱数のビット長、暗号化アルゴリズムについては上記に説明したもの限定されない。

(10) 暗号化部 315

暗号化部 315 は、装置固有鍵生成部 317 から装置固有鍵を受け取り、復号部 314 からソフトウェアを受け取る。

【0072】

次に、暗号化部 315 は、受け取った装置固有鍵を用いて、受け取ったソフトウェアに暗号化アルゴリズム E2 を施して、暗号化ソフトウェアを生成する。

ここで、暗号化アルゴリズム E2 は、DES により規定されたものである。

次に、暗号化部 315 は、生成した暗号化ソフトウェアをソフトウェア格納部 320 へ書き込む。

【0073】

(11) 復号部 325

復号部 325 は、装置固有鍵生成部 317 から装置固有鍵を受け取る。また、復号部 325 は、利用者の指示により、ソフトウェア格納部 320 から暗号化ソフトウェアを読み出す。次に、復号部 325 は、受け取った装置固有鍵を用いて、読み出した暗号化ソフトウェアに復号アルゴリズム D2 を施して、ソフトウェアを生成する。

【0074】

ここで、復号アルゴリズム D2 は、DES により規定されたものであり、暗号化アルゴリズム E2 に対応するものである。復号アルゴリズム D2 は、暗号化アルゴリズム E2 を用いて生成された暗号文を復号する。

次に、復号部 325 は、生成したソフトウェアをソフトウェア実行部 324 へ出力する。

【0075】

(12) ソフトウェア実行部 324

ソフトウェア実行部 324 は、復号部 325 からソフトウェアを受け取り、受け取ったソフトウェアに従って動作する。

(13) 制御部 321

制御部 321 は、情報処理装置 300 を構成する各構成部を制御する。

【0076】

アンインストールの際には、制御部 321 は、復号部 313 から、アンインストール可否情報及び乱数 R' を受け取り、受け取ったアンインストール可否情報を用いて、アンインストールの可否を判断する。

アンインストールが不可であると判断する場合に、制御部 321 は、アンインストール処理を行わず、アンインストールが未完了であることを示す 8 ビット長の完了情報を生成する。

【0077】

アンインストールが可であると判断する場合に、制御部 321 は、ソフトウェア格納部 320 に格納されている暗号化ソフトウェアが実行できないように暗号化ソフトウェアを非活性化処理することにより、該ソフトウェアをアンインストールする。

ここでソフトウェアを非活性化処理するためには、例えば、乱数格納部 326 に格納されている乱数を他の乱数に更新する。

【0078】

次に、制御部 321 は、ソフトウェアのアンインストールが完了したことを示す 8 ビット長の完了情報を生成し、生成した完了情報及び乱数 R' を暗号化部 312 へ出力する。

(14) 入力部 323

入力部 323 は、利用者から入力を受け付ける。具体的には、情報処理装置 300 にメモ리카ード 200 が装着されると、入力部 323 は、利用者からソフトウェアのインストール又はアンインストールを示す区分を受け付け、受け付けた区分を制御部 321 を介して、暗号化部 312 へ出力する。

【0079】

インストールを示す区分を受け付けた場合には、入力部 323 は、さらに、利用者からインストールするソフトウェアの指定を受け付ける。一方、アンインストールを示す区分を受け付けた場合には、入力部 323 は、利用者からアンインストールする暗号化ソフトウェアの指定を受け付ける。

(15) 表示部 322

表示部 322 は、制御部 321 の制御により、各種情報を表示する。具体的には、入力部 323 がインストールを示す区分を受け付けた場合には、表示部 322 は、メモ리카ード 200 に記憶されているソフトウェアの一覧を表示する。一方、入力部 323 がアンインストールを示す区分を受け付けた場合には、表示部 322 は、情報処理装置 300 のソフトウェア格納部 320 に格納されている暗号化ソフトウェアの一覧を表示する。

【0080】

1. 5 ソフトウェア管理システム 10 の動作

利用者が情報処理装置 300 にメモ리카ード 200 を装着した後に、メモ리카ード 200 に記憶されているソフトウェアを情報処理装置 300 へインストールする場合及び情報処理装置 300 に既にインストールされている暗号化ソフトウェアをアンインストールする場合のソフトウェア管理システム 10 の動作について、図 5～9 に示すフローチャートを用いて説明する。

【0081】

情報処理装置 300 にメモ리카ード 200 が装着されると、入力部 323 は、利用者からソフトウェアのインストール又はアンインストールを示す区分を受け付け、受け付けた区分を制御部 321 を介して、暗号化部 312 へ出力し、入力部 323 がインストールを示す区分を受け付けた場合には、表示部 322 は、メモ리카ード 200 に記憶されているソフトウェアの一覧を表示し、入力部 323 は、利用者からインストールするソフトウェアの指定を受け付け、入力部 323 がアンインストールを示す区分を受け付けた場合には、表示部 322 は、情報処理装置 300 のソフトウェア格納部 320 に格納されている暗号化ソフトウェアの一覧を表示し、入力部 323 は、利用者からアンインストールする暗号化ソフトウェアの指定を受け付ける（ステップ S100）。

【0082】

情報処理装置 300 は、ソフトウェア又は暗号化ソフトウェアの指定を受け付けると、情報処理装置 300 が有する認証部 311 とメモ리카ード 200 が有する認証部 211 との間で、相互に認証を行う（ステップ S101、ステップ S102）。

認証に成功すると（ステップ S104）、暗号化部 312 は、認証部 311 よりセッション鍵を受け取り、ソフト ID 取得部 318 よりソフト ID を受け取り、装置 ID 格納部より装置 ID を読み出し、受け取ったセッション鍵を用いて、区分、ソフト ID 及び装置 ID を暗号化して暗号化区分、暗号化ソフト ID 及び暗号化装置 ID を生成し（ステップ S105）、生成した暗号化区分、暗号化ソフト ID 及び暗号化装置 ID をメモ리카ード 200 に送信する（ステップ S106）。

【0083】

認証に成功すると（ステップS103）、復号部212は、認証部211よりセッション鍵を受け取り、受け取ったセッション鍵を用いて、情報処理装置300より受信した暗号化区分、暗号化ソフトID及び暗号化装置IDを復号し、生成した区分、ソフトID及び装置IDを判定部214に送る（ステップS107）。

【0084】

認証に失敗すると（ステップS103又はS104）、メモリカード200又は情報処理装置300は、以降の処理を中止する。

次に、判定部214は、第2記憶領域222から、前記生成されたソフトIDに対応するソフトウェア管理情報を読み出し（ステップS108）、生成された区分がソフトウェアのインストール又はアンインストールのいずれを示すかを判断する（ステップS109）。

【0085】

（インストール時の処理）

区分がソフトウェアのインストールを示すと判断する場合に（ステップS109）、判定部214は、読み出したソフトウェア管理情報に基づいて、インストールを許可するか否かを判定する（ステップS110）。なおステップS110の詳細は後述する。

【0086】

インストールを許可しないと判定した場合に（ステップS110）、判定部214は、不許可を示す不許可メッセージを情報処理装置300に送信し（ステップS120）、その後、メモリカード200は、処理を中止する。

メモリカード200から前記不許可メッセージを受け取ると（ステップS121）、制御部321は、表示部322に対して前記不許可メッセージを表示するように制御し、表示部322は、前記不許可メッセージを表示し（ステップS122）、その後、情報処理装置300は、処理を中止する。

【0087】

インストールを許可すると判定した場合に（ステップS110）、判定部214は、ソフト管理情報に含まれるソフトキーを暗号化部213に送り、暗号化部

213は、ソフトキーを、認証部211より受け取ったセッション鍵を用いて暗号化して暗号化ソフトキーを生成し（ステップS111）、生成した暗号化ソフトキーを情報処理装置300に送信し（ステップS112）、制御部321が前記不許可メッセージを受け取っていない場合に（ステップS121）、復号部313は、メモリカード200から受け取った暗号化ソフトキーを、認証部311より受け取ったセッション鍵を用いて復号する（ステップS113）。

【0088】

また、第1記憶領域221から暗号化ソフトウェアが読み出され（ステップS114）、読み出された暗号化ソフトウェアが情報処理装置300へ送信される（ステップS115）。復号部314は、復号部313から受取った復号されたソフトキーを用いて、暗号化ソフトウェアを復号し（ステップS116）、復号されたソフトウェアを暗号化部315へ送り、装置固有鍵生成部317は、装置ID格納部316より装置IDを読み出し、読み出した装置IDを用いて装置固有鍵を生成し（ステップS117）、暗号化部315は、復号部314より受け取ったソフトウェアを、装置固有鍵生成部317より受け取った装置固有鍵を用いて暗号化して暗号化ソフトウェアを生成し（ステップS118）、暗号化部315は、生成した暗号化ソフトウェアをソフトウェア格納部320に書き込むことにより、インストールする（ステップS119）。

【0089】

以上のようにして、暗号化ソフトウェアのインストールが完了する。

（アンインストール時の処理）

区分がソフトウェアのアンインストールを示すと判断する場合に（ステップS109）、さらに、判定部214は、復号部212から受け取った装置IDが、第2記憶領域222から読み出したソフトウェア管理情報に含まれるかどうかを判断し、装置IDが含まれない場合は（ステップS201）、アンインストール不可と判定してアンインストール不可を示す8ビット長のアンインストール可否情報を生成する（ステップS203）。一方、装置IDが含まれる場合は（ステップS201）、判定部214は、アンインストール可と判定してアンインストール可を示す8ビット長のアンインストール可否情報を生成する（ステップS2

02)。

【0090】

次に、判定部214は、56ビット長の乱数Rを生成し、生成した乱数Rを保持し（ステップS204）、生成した乱数R及びアンインストールの可否を示すアンインストール可否情報を暗号化部213へ出力し、暗号化部213は、乱数R及びアンインストール可否情報を受け取り、認証部211から受け取ったセッション鍵を用いて、受け取った乱数R及びアンインストール可否情報に暗号化アルゴリズムE4を施して、暗号化アンインストール可否情報を生成し（ステップS205）、生成した暗号化アンインストール可否情報を情報処理装置300へ出力する（ステップS206）。

【0091】

復号部313は、メモ리카ード200から暗号化アンインストール可否情報を受け取り（ステップS206）、認証部311から受け取ったセッション鍵を用いて、受け取った暗号化アンインストール可否情報に復号アルゴリズムD4を施して、アンインストール可否情報及び乱数R'を生成し、生成したアンインストール可否情報及び乱数R'を制御部321へ出力する（ステップS207）。

【0092】

次に、制御部321は、アンインストール可否情報及び乱数R'を受け取り、受け取ったアンインストール可否情報を用いて、アンインストールの可否を判断し、アンインストールが不可であると判断する場合に（ステップS208）、アンインストール処理を行わず、アンインストールが未完了であることを示す8ビット長の完了情報を生成し（ステップS211）、次に、ステップS212へ制御を移す。

【0093】

アンインストールが可であると判断する場合に（ステップS208）、制御部321は、ソフトウェア格納部320に格納されている暗号化ソフトウェアが実行できないように暗号化ソフトウェアを非活性化処理することにより、該ソフトウェアをアンインストールする。ここでソフトウェアを非活性化処理するためには、例えば、乱数格納部326に格納されている乱数を他の乱数に更新すればよ

い（ステップS209）。次に、制御部321は、ソフトウェアのアンインストールが完了したことを示す8ビット長の完了情報を生成する（ステップS210）。

【0094】

次に、制御部321は、完了情報及び乱数R'を暗号化部312へ出力し、暗号化部312は、完了情報及び乱数R'を受け取り、認証部311から受け取ったセッション鍵を用いて、受け取った完了情報及び乱数R'に暗号化アルゴリズムE3を施して、暗号化完了情報を生成し（ステップS212）、生成した暗号化完了情報を、復号部212へ出力する（ステップS213）。

【0095】

復号部212は、暗号化部312から暗号化完了情報を受け取り（ステップS213）、認証部211から受け取ったセッション鍵を用いて、受け取った暗号化完了情報に復号アルゴリズムD3を施して、完了情報及び乱数R'を生成し、生成した完了情報及び乱数R'を判定部214へ出力する（ステップS214）。

【0096】

次に、判定部214は、完了情報及び乱数R'を受け取り、受け取った乱数R'と保持している乱数Rとが一致するか否かを判断し、一致しない場合には（ステップS215）、アンインストール処理を中止する。

一致する場合には（ステップS215）、判定部214は、さらに、完了情報がアンインストールが完了したことを示しているか否かを判断し、完了情報がアンインストールが完了したことを示していない場合は（ステップS216）、以降のアンインストール処理を中止する。

【0097】

一方、完了情報がアンインストールが完了したことを示している場合は、（ステップS216）、判定部214は、ソフトウェア管理情報に含まれるインストール回数情報に「1」の値を加算し、得られた値を、新たにインストール回数情報として、ソフトウェア管理テーブル231内の前記ソフトウェア管理情報内に上書きする（ステップS217）。

【0098】

このようにして、アンインストールが完了する。

以上で説明したアンインストールの手順を利用すれば、例えば、利用者が、暗号化ソフトウェアをインストールしていたハードディスクユニットを、新規のハードディスクユニットに交換したいような場合に、メモリカードに記録されているインストール回数情報が、例え「0」を示している場合であっても、アンインストールを実行することにより新規のハードディスクユニットに新たにインストールすることが可能となる。

【0099】

なお、複数の暗号化ソフトウェアがソフトウェア格納部 320 にインストールされている場合は、前記ステップ S 209 において、前記乱数格納部 326 に格納されている乱数を更新する前に、アンインストール対象の暗号化ソフトウェア以外の暗号化ソフトウェアに対して、復号部 325 で、更新前の乱数より生成される装置固有鍵を用いて復号してソフトウェアを生成し、生成したソフトウェアを、暗号化部 315 で更新後の乱数より生成される装置固有鍵を用いて、再び暗号化して再暗号化ソフトウェアを生成し、生成した再暗号化ソフトウェアをソフトウェア格納部 320 に格納すればよい（ステップ S 209 a）。

【0100】

（ステップ 110 の詳細の動作）

次に、判定部 214 における前記ステップ 110 の詳細の動作について、図 9 に示すフローチャートを用いて説明する。

判定部 214 は、復号部 212 より受け取った装置 ID が、第 2 記憶領域 222 より受取ったソフトウェア管理情報に含まれるかどうかチェックし（ステップ S 151）、装置 ID が含まれない場合は（ステップ S 151）、新しい情報処理装置へのインストールの要請と判断し、ソフトウェア管理情報に含まれるインストール回数をチェックし（ステップ S 153）、1 以上であれば（ステップ S 153）インストール可と判定する。このとき、前記第 2 記憶領域 222 より読み出したソフトウェア管理情報に、前記復号部 212 より受け取った装置 ID を追加して書き込むとともに、インストール回数を 1 減算した値に更新したソフト

ウェア管理情報を第2記憶領域222に書き込む(ステップS155)。インストール回数が零であれば(ステップS153)、インストール不可と判定する。また、前記ステップ151において、装置IDが含まれる場合は(ステップS151)、既にインストール済みの情報処理装置への再インストールの要請と判断し、インストール可と判定する。

【0101】

なお、ソフトウェア管理情報は、インストール期間情報を含むとしてもよい。ここで、インストール期間情報は、64ビット長であり、利用者に対して、当該ソフトウェア管理情報に対応するソフトウェアをインストールすることができる期間を制限するものであり、インストール期間の開始日時を示すインストール許可開始日時と、インストール期間の終了日時を示すインストール許可終了日時とから構成される。利用者に対して、インストール許可開始日時からインストール許可終了日時までの期間内においてのみ、当該ソフトウェアのインストールが許可される。この期間内であれば、利用者は、当該ソフトウェアを何回でもインストールすることができる。ここで、インストール期間情報とインストール回数情報の両方が指定されている場合には、許可されている期間が終了するか、インストール回数までインストールした後には、ソフトウェアをインストールすることはできないものとする。

【0102】

1. 6 その他の例

ソフトウェア管理システム10は、以下のように構成してもよい。

(1) 実施の形態1においては、ソフトウェア書込装置100は、パーソナルコンピュータ等で構成されるコンピュータシステムとしているが、この構成に限定されるものではない。例えば、ソフトウェア書込装置100は、KIOSK端末により構成されとしても良い。

【0103】

(2) 実施の形態1では、ソフトウェアの書き込まれたメモリカード200は、利用者に提供されとしているが、この構成に限定されるものではない。

ソフトウェアの書き込まれたメモリカード200は、ソフトウェア販売店やC

E 機器メーカーの顧客サービスセンターのサービスマンに提供され、このサービスマンにより、利用者の情報処理装置にメモ리카ード 2 0 0 が挿入されるとしても良い。

【0 1 0 4】

(3) 実施の形態 1 では、ソフトウェア書込装置 1 0 0 がメモ리카ード 2 0 0 にソフトウェア管理情報を書き込む時点においては、ソフトウェア管理情報 2 4 1 は、装置 ID を含まないとしているが、この構成に限定されるものではない。

ソフトウェア書込装置 1 0 0 がメモ리카ード 2 0 0 にソフトウェア管理情報を書き込む時点において、ソフトウェア管理情報 2 4 1 は、装置 ID を含んでいるとしても良い。

【0 1 0 5】

このように構成することにより、利用者が提供されたメモ리카ードを用いて初めてソフトウェアをインストールする際に、ソフトウェア提供者は、利用者に対して、ソフトウェアをインストールする情報処理装置を限定できる。

(4) 実施の形態 1 では、ソフトウェアをインストールする際に、復号部 3 1 4 は、ソフトキーを用いて、メモ리카ード 2 0 0 から受け取った暗号化ソフトウェアを復号し（ステップ S 1 1 6）、暗号化部 3 1 5 は、装置固有鍵を用いて、復号されたソフトウェアを暗号化し（ステップ S 1 1 7 ~ S 1 1 8）、生成した暗号化ソフトウェアをソフトウェア格納部 3 2 0 に書き込むことによりソフトウェアをインストールする（ステップ S 1 1 9）としているが、この構成に限定されるものではない。

【0 1 0 6】

装置固有鍵生成部 3 1 7 は、装置固有鍵を生成し（ステップ S 1 1 7）、暗号化部 3 1 5 は、生成された装置固有鍵を用いて、復号部 3 1 3 から受け取ったソフトキーを暗号化して暗号化ソフトキーを生成し（ステップ S 1 1 8'）、生成した暗号化ソフトキーと、メモ리카ード 2 0 0 から受け取った暗号化ソフトウェアをソフトウェア格納部 3 2 0 に書き込むことによりインストールする（ステップ S 1 1 9'）ように構成にしても良い。

【0 1 0 7】

このとき、情報処理装置 300 は、さらに復号部 327 (図示していない) を備え、ソフトウェアの実行時には、復号部 325 は、受け取った装置固有鍵を用いて、暗号化ソフトキーを復号してソフトキーを生成し、生成したソフトキーを復号部 327 へ出力し、復号部 327 は、復号部 325 からソフトキーを受け取り、受け取ったソフトキーを用いて、暗号化ソフトウェアを復号してソフトウェアを生成し、生成したソフトウェアをソフトウェア実行部 324 へ出力する。ソフトウェア実行部 324 は、復号部 327 からソフトウェアを受け取り、受け取ったソフトウェアに従って、ソフトウェア実行部 324 は、動作する。

【0108】

(5) 実施の形態 1 では、インストール時及びソフトウェア実行時において、装置固有鍵生成部 317 は、乱数格納部 326 から 64 ビット長の乱数を読み出すものとし、アンインストール時において、乱数格納部 326 の前記乱数を更新するとしているが、この構成に限定されるものではない。

乱数格納部 326 は、インストールするソフトウェアに対応付けて、64 ビット長の乱数を記憶しており、インストール時及びソフトウェア実行時において、乱数格納部 326 から、インストールするソフトウェアに対応する 64 ビット長の乱数を読み出すものとし、アンインストール時において、乱数格納部 326 の前記ソフトウェアに対応する乱数を更新する構成としても良い。

【0109】

この構成により、前記ステップ S209 において、複数の暗号化ソフトウェアがソフトウェア格納部 320 にインストールされている場合において、実施の形態 1 で必要であった暗号化ソフトウェアの復号、再暗号化処理 (ステップ S209a) は不要となる。

(6) 実施の形態 1 では、認証の方法としてチャレンジレスポンス型の認証を挙げ、セッション鍵の共有方法として、チャレンジレスポンス型の認証のプロセスにおいて使用される乱数情報に基づいてセッション鍵を生成することにより行うものとしているが、この構成に限定されるものではない。

【0110】

例えば認証の方法として、デジタル署名を利用する方法を利用し、セッション

鍵の共有方法としては、ディフィーヘルマン (DH) 型鍵共有方法を利用しても良い。

デジタル署名を利用する認証方法については、「現代暗号理論」(池野信一、小山謙二共著、電子情報通信学会)、P 83, 5. 3, (2) に、また、DH 型鍵共有方法については、同 P 175 に詳細に説明されている。

【0111】

(7) 実施の形態 1 では、ソフトウェアをソフトウェア書込装置がメモ리카ードに書き込む際に、ソフトキーは、予めソフトウェア管理情報に含まれるものとし、暗号化部 112 により、ソフトウェア管理テーブル 121 から、前記ソフト ID を含むソフトウェア管理情報を読み出し、読み出したソフトウェア管理情報からソフトキーを抽出するものとしたが、この構成に限定されるものではない。

【0112】

例えば、ソフトキーは、ソフトウェア管理情報に含まれないものとし、暗号化部 112 は、ソフトウェア管理テーブル 121 から、前記ソフト ID を含むソフトウェア管理情報を読み出すとともに、ソフトキーを生成するものとしても良い。

(8) 実施の形態 1 では、アンインストール処理において、アンインストール可否情報と、完了情報をそれぞれ 8 ビットとし、乱数 R を 56 ビットとしたがこれらのビット長に限定されるものではない。

【0113】

(9) 実施の形態 1 では、アンインストール処理のステップ S 212 において、セッション鍵を用いて、完了情報及び乱数 R' に暗号化アルゴリズム E 3 を施すとしたが、この構成に限定されるものではない。

例えば、完了情報、及び、乱数 R' のビット反転値 (R'') に、暗号化アルゴリズム E 3 を施すとしてもよい。この場合、ステップ S 215 においては、受け取った乱数 R'' と、保持している乱数 R のビット反転値が一致するか否かを判断するものとする。

【0114】

(10) 実施の形態 1 では、ソフトウェアは、コンピュータプログラムなどで

あるとしているが、コンピュータプログラムの動作に付随するデータであっても良い。

(11) 実施の形態1のソフトウェア管理テーブルに、機種ID(グループID)を含める構成としても良い。ここで、機種ID(グループID)は、情報処理装置の種類を識別する識別情報である。また、同一の種類の情報処理装置とは、例えば、同一の処理性能を有するマイクロプロセッサを内蔵するもの、同一の容量のハードディスクを内蔵するもの、同一の容量のメモリを内蔵するもの、同一メーカーにより製造されたものなどを言う。

【0115】

この場合、情報処理装置は、自身の種類を識別する機種ID(グループID)を備え、メモリカードは、機種ID(グループID)に基づいて、同一機種(同一グループ)へのインストール、アンインストールの判定を行う。この構成によりインストールを特定機種の情報処理装置に限定することも可能である

(12) 実施の形態1のソフトウェア管理テーブルに、ソフトウェアのバージョン情報を含める構成としても良い。

【0116】

この場合、情報処理装置において、インストール対象のソフトIDとともに、バージョン情報を受け付け、メモリカードでは、ソフトIDとともに、バージョン情報に基づいて、インストールやアンインストールの可否の判定や、該バージョンのソフトウェアのインストールやアンインストールを行う。

(13) 実施の形態1では、メモリカードの第1記憶領域に暗号化ソフトウェアを記憶する構成としたが、これに限定されるものではない。

【0117】

暗号化ソフトウェアを、別途、通信回線や、別の記録媒体を介して、情報処理装置が取得する構成としても良い。

2. 変形例(1)

実施の形態1の変形例としてのソフトウェア管理システム10b(図示していない)について説明する。

【0118】

ソフトウェア管理システム 10b は、ソフトウェア書込装置 100b、可搬型のメモリカード 200b 及び情報処理装置 300b から構成されている。ソフトウェア書込装置 100b、メモリカード 200b 及び情報処理装置 300b は、それぞれソフトウェア書込装置 100、メモリカード 200 及び情報処理装置 300 と同様の構成を有している。

【0119】

ここでは、ソフトウェア書込装置 100、メモリカード 200 及び情報処理装置 300 との相違点を中心として、ソフトウェア書込装置 100b、メモリカード 200b 及び情報処理装置 300b について説明する。

2. 1 ソフトウェア書込装置 100b の構成

ソフトウェア書込装置 100b は、図 10 に示すように、認証部 111、暗号化部 112、情報記憶部 113、制御部 114、署名生成部 117 及び入出力部 118 から構成されている。また、ソフトウェア書込装置 100b には、入力部 115 及び表示部 116 が接続されている。

【0120】

このように、ソフトウェア書込装置 100b は、ソフトウェア書込装置 100 と同様の構成を有しており、ソフトウェア書込装置 100b は、さらに、署名生成部 117 を備えている点において、ソフトウェア書込装置 100 と相違する。

(1) 署名生成部 117

署名生成部 117 は、暗号化部 112 から暗号化ソフトウェアを受け取る。暗号化ソフトウェアを受け取ると、署名生成部 117 は、受け取った暗号化ソフトウェアに、デジタル署名生成アルゴリズム SIG を施して、ソフト署名データを生成する。

【0121】

ここで、デジタル署名生成アルゴリズム SIG は、160 ビット長の楕円曲線暗号によるデジタル署名の生成法に基づくものであり、ソフト署名データは、320 ビット長である。なお、楕円曲線暗号については、「暗号理論の基礎」(Douglas R. Stinson 著、共立出版株式会社) に詳細に説明されている。

【0122】

次に、署名生成部 117 は、生成したソフト署名データをメモリカード 200b の判定部 214 へ出力する。

2. 2 メモリカード 200b の構成

メモリカード 200b は、図 10 及び図 12 に示すように、耐タンパモジュール部 210 及び情報記憶部 220 から構成されている。耐タンパモジュール部 210 及び情報記憶部 220 は、メモリカード 200 が有する耐タンパモジュール部 210 及び情報記憶部 220 と同様の構成を有している。

【0123】

ここでは、メモリカード 200 との相違点を中心として説明する。

(1) 判定部 214

判定部 214 は、認証部 211 から第 1 認証成功情報を受け取ると、さらに、ソフト署名データを受け取る。次に、判定部 214 は、受け取ったソフト署名データを、受け取ったソフトウェア管理情報内に書き込み、ソフト署名データを含むソフトウェア管理情報をソフトウェア管理情報テーブル 231 内に追加して書き込む。

【0124】

ソフト署名データが書き込まれたソフトウェア管理情報の一例を図 11 に示す。この図に示すソフトウェア管理情報 241b は、ソフト ID、ソフトキー、インストール回数情報、ソフト署名データ及び複数の装置 ID を含む。

なお、図 11 に示すソフトウェア管理情報 241b は、複数の装置 ID を含むように構成されているが、ソフトウェア書込装置 100 からメモリカード 200 に、ソフトウェア管理情報が書き込まれる時点においては、まだ、ソフトウェア管理情報 241b は、複数の装置 ID を含んでいないものとする。

【0125】

判定部 214 が第 2 認証成功情報を受け取った場合であって、インストールを許可すると判定したときに、受け取ったソフト署名データを情報処理装置 300b へ出力する。

2. 3 情報処理装置 300b の構成

情報処理装置 300b は、図 12 に示すように、インストール処理部 310、ソフトウェア格納部 320、制御部 321、表示部 322、入力部 323、ソフトウェア実行部 324 及び復号部 325 から構成されている。インストール処理部 310 は、さらに、認証部 311、暗号化部 312、復号部 313、復号部 314、暗号化部 315、装置 ID 格納部 316、装置固有鍵生成部 317、ソフト ID 取得部 318 及び署名検証部 319 から構成されている。

【0126】

このように、情報処理装置 300b は、情報処理装置 300 と同様の構成を有しており、さらに署名検証部 319 を備えている点において、情報処理装置 300 と異なる。

(1) 署名検証部 319

署名検証部 319 は、メモリカード 200b の判定部 214 からソフトウェア管理情報に含まれるソフト署名データを受け取る。また、署名検証部 319 は、メモリカード 200b の第 1 記憶領域 221 から暗号化ソフトウェアを読み出す。

【0127】

次に、署名検証部 319 は、受け取ったソフト署名データ及び読み出した暗号化ソフトウェアに、デジタル署名検証アルゴリズム VRF を施し、検証成功を示す検証成功情報、又は検証失敗を示す検証失敗情報を生成する。

ここで、デジタル署名検証アルゴリズム VRF は、楕円暗号によるデジタル署名の検証法に基づくものである。

【0128】

次に、署名検証部 319 は、検証成功情報又は検証失敗情報を復号部 314 へ出力する。

(2) 復号部 314

復号部 314 は、署名検証部 319 から検証成功情報又は検証失敗情報を受け取る。

【0129】

検証失敗情報を受け取ると、復号部 314 は、以降の復号処理を中止する。

検証成功情報を受け取ると、復号部 314 は、暗号化ソフトウェアの復号を継続して行う。

2. 4 その他の例

(1) 変形例 (1) において、署名生成部 117 は、暗号化ソフトウェアにデジタル署名生成アルゴリズム SIG を施してソフト署名データを生成するとしているが、この構成には限定されない。

【0130】

署名生成部 117 は、暗号化ソフトウェアとソフトキーとインストール回数情報とにデジタル署名生成アルゴリズム SIG を施してソフト署名データを生成するとしてもよい。

この場合、ソフトウェアのインストール時に、暗号化部 213 は、セッション鍵を用いて、ソフトキー及びインストール回数情報を暗号化して暗号化情報を生成し、生成した暗号化情報を情報処理装置 300b へ送信する。情報処理装置 300b の復号部 313 は、セッション鍵を用いて、受け取った暗号化情報を復号して、ソフトキー及びインストール回数情報を生成し、署名検証部 319 は、ソフト署名データ、暗号化ソフトウェア、生成されたソフトキー及び生成されたインストール回数情報に、署名検証アルゴリズム VRF を施して、ソフト署名データを検証するものとする。

【0131】

また、署名生成部 117 は、ソフトウェアにデジタル署名アルゴリズム SIG を施してソフト署名データを生成するとしても良い。

この場合、インストール時に、署名検証部 319 は、ソフト署名データと、前記ソフトウェアに、署名検証アルゴリズム VRF を施して、ソフト署名データを検証するものとする。なお、この場合、メモ리카ード 200b の第 1 記憶領域 221 には、暗号化されていないソフトウェアが書き込まれる。

【0132】

3. 変形例 (2)

ソフトウェア管理システム 10b の変形例としてのソフトウェア管理システム 10c (図示していない) について説明する。

ソフトウェア管理システム 10c は、ソフトウェア書込装置 100c (図示していない)、可搬型のメモリカード 200c 及び情報処理装置 300c から構成されている。ソフトウェア書込装置 100c は、ソフトウェア書込装置 100b と同一の構成を有している。メモリカード 200c 及び情報処理装置 300c は、それぞれメモリカード 200b 及び情報処理装置 300b と同様の構成を有している。

【0133】

ここでは、メモリカード 200b 及び情報処理装置 300b との相違点を中心として、メモリカード 200c 及び情報処理装置 300c について説明する。

3. 1 メモリカード 200c の構成

メモリカード 200c は、図 13 に示すように、耐タンパモジュール部 210 及び情報記憶部 220 から構成されている。耐タンパモジュール部 210 及び情報記憶部 220 は、メモリカード 200b が有する耐タンパモジュール部 210 及び情報記憶部 220 と同様の構成を有している。

【0134】

ここでは、メモリカード 200b との相違点を中心として説明する。

耐タンパモジュール部 210 は、認証部 211、復号部 212、暗号化部 213 及び判定部 214、復号部 215、暗号化部 216 及びキー情報記憶部 217 から構成されている。このように、耐タンパモジュール部 210 は、さらに、復号部 215、暗号化部 216 及びキー情報記憶部 217 を備える点において、メモリカード 200b の耐タンパモジュール部 210 と相違する。

【0135】

(1) 判定部 214

判定部 214 は、認証部 211 から第 1 認証成功情報を受け取ると、さらに、ソフト署名データを受け取る。次に、判定部 214 は、受け取ったソフト署名データを、受け取ったソフトウェア管理情報内に書き込み、次に、ソフト署名データを含むソフトウェア管理情報を暗号化部 216 へ出力する。

【0136】

ソフト署名データが書き込まれたソフトウェア管理情報の一例は、図 11 に示

す通りである。

また、判定部 214 は、復号部 215 からソフトウェア管理情報を受け取る。

(2) キー情報記憶部 217

キー情報記憶部 217 は、キー情報を記憶している。キー情報は、56 ビット長のデータであり、ソフトウェア管理情報を暗号化又は復号するために用いられる。

【0137】

(3) 暗号化部 216

暗号化部 216 は、判定部 214 からソフトウェア管理情報を受け取り、キー情報記憶部 217 からキー情報を読み出す。

次に、暗号化部 216 は、読み出したキー情報を用いて、受け取ったソフトウェア管理情報に暗号化アルゴリズム E5 を施して、暗号化ソフトウェア管理情報を生成し、生成した暗号化ソフトウェア管理情報を第 2 記憶領域 222 が有する暗号化ソフトウェア管理情報テーブル 231c に書き込む。

【0138】

ここで、暗号化アルゴリズム E5 は、DES により規定されたものである。

(4) 復号部 215

復号部 215 は、第 2 記憶領域 222 が有する暗号化ソフトウェア管理情報テーブル 231c から暗号化ソフトウェア管理情報を読み出し、キー情報記憶部 217 からキー情報を読み出す。

【0139】

次に、復号部 215 は、読み出したキー情報を用いて、読み出した暗号化ソフトウェア管理情報に復号アルゴリズム D5 を施して、ソフトウェア管理情報を生成し、生成したソフトウェア管理情報を判定部 214 へ出力する。

ここで、復号アルゴリズム D5 は、DES により規定されたものであり、暗号化アルゴリズム E5 に対応するものである。復号アルゴリズム D5 は、暗号化アルゴリズム E5 を用いて生成された暗号文を復号する。

【0140】

3. 2 情報処理装置 300c の構成

情報処理装置 300c は、図 13 に示すように、インストール処理部 310、ソフトウェア格納部 320、制御部 321、表示部 322、入力部 323、ソフトウェア実行部 324 及び復号部 325 から構成されている。インストール処理部 310 は、さらに、認証部 311、暗号化部 312、復号部 313、復号部 314、暗号化部 315、装置 ID 格納部 316、装置固有鍵生成部 317、ソフト ID 取得部 318 及び署名検証部 319 から構成されている。

【0141】

このように、情報処理装置 300c は、情報処理装置 300b と同様の構成を有しているので、詳細についての説明を省略する。

3. 3 その他の例

変形例 (2) では、キー情報記憶部 217 に記憶されているキー情報は固定値であるとしているが、これに限定されることなく、キー情報は、可変値であるとしてもよい。

【0142】

この場合、第 2 記憶領域 222 から判定部 214 へソフトウェア管理情報を出力する際に、復号部 215 は、暗号化ソフトウェア管理テーブル 231c から全ての暗号化ソフトウェア管理情報を読み出し、キー情報記憶部 217 からキー情報を読み出し、次に復号部 215 は、読み出したキー情報を用いて読み出した全暗号化ソフトウェア管理情報に復号アルゴリズム D5 を施してソフトウェア管理情報を生成する。次に、判定部 214 から第 2 記憶領域 222 へソフトウェア管理情報を出力する際に、判定部 214 は、キー情報を更新してキー情報記憶部 217 に格納し、暗号化部 216 は、更新されたキー情報を用いて、復号された全ソフトウェア管理情報に、暗号化アルゴリズム E5 を施して暗号化ソフトウェア管理情報を生成し、第 2 記憶領域 222 の暗号化ソフトウェア管理テーブル 231c に書き込むとしても良い。

【0143】

4. 変形例 (3)

変形例 (1) に示すソフトウェア管理システム 10b の変形例としてのソフトウェア管理システム 10d (図示していない) について説明する。

ソフトウェア管理システム 10d は、ソフトウェア書込装置 100d (図示していない)、可搬型のメモリカード 200d 及び情報処理装置 300d から構成されている。ソフトウェア書込装置 100d、メモリカード 200d 及び情報処理装置 300d は、それぞれソフトウェア書込装置 100b、メモリカード 200b 及び情報処理装置 300b と同様の構成を有している。

【0144】

ここでは、メモリカード 200b との相違点を中心として、メモリカード 200d について説明する。

メモリカード 200d は、図 14 に示すように、耐タンパモジュール部 210 及び情報記憶部 220 から構成されている。耐タンパモジュール部 210 は、認証部 211、復号部 212、暗号化部 213、判定部 214 及び情報記憶部 218 から構成されている。メモリカード 200b が有する耐タンパモジュール部 210 とは、メモリカード 200d が有する耐タンパモジュール部 210 がさらに情報記憶部 218 を有している点において、相違している。

【0145】

(1) 情報記憶部 218

情報記憶部 218 は、図 15 に一例として示す部分ソフトウェア管理テーブル 219 を有している。

部分ソフトウェア管理テーブル 219 は、複数の部分ソフトウェア管理情報を記憶するための領域を備えている。各部分ソフトウェア管理情報は、ソフト ID 及び前半ソフト署名データから構成されている。

【0146】

ここで、ソフト ID については、上述した通りであるので、説明を省略する。

前半ソフト署名データは、上述したソフト署名データを構成するビット列のうち、前半の部分のビット列から構成されている。具体的には、前半ソフト署名データは、160 ビット長のビット列から構成されている。

(2) ソフトウェア管理情報テーブル 231

ソフトウェア管理情報テーブル 231 は、図 15 に示すように、一例として、ソフトウェア管理情報 241d、・・・を記憶するための領域を備えている。

【0147】

ソフトウェア管理情報 241d は、ソフト ID、ソフトキー、インストール回数情報、後半ソフト署名データ、及び複数の装置 ID を含んでいる。

ここで、ソフト ID、ソフトキー、インストール回数情報及び複数の装置 ID については、上述した通りであるので説明を省略する。

後半ソフト署名データは、上述したソフト署名データを構成するビット列のうち、後半の部分のビット列から構成されている。具体的には、後半ソフト署名データは、160ビット長のビット列から構成されている。

【0148】**(3) 判定部 214**

判定部 214 は、認証部 211 から第 1 認証成功情報を受け取ると、さらに、ソフト署名データを受け取る。次に、判定部 214 は、受け取ったソフト署名データを、2 個のビット列に分割して、前半ソフト署名データ及び後半ソフト署名データを生成する。分割して生成された前半のビット列が前半ソフト署名データであり、後半のビット列が後半ソフト署名データである。前半ソフト署名データ及び後半ソフト署名データは、それぞれ、160ビット長である。

【0149】

次に、判定部 214 は、生成した前半ソフト署名データ及び受け取ったソフト ID から構成される部分ソフトウェア管理情報を生成し、生成した部分ソフトウェア管理情報を情報記憶部 218 が有する部分ソフトウェア管理テーブル 219 内に書き込む。また、判定部 214 は、生成した後半ソフト署名データを含むソフトウェア管理情報をソフトウェア管理情報テーブル 231 内に追加して書き込む。

【0150】

また、判定部 214 は、部分ソフトウェア管理テーブル 219 から、ソフト ID を含む部分ソフトウェア管理情報を読み出し、ソフトウェア管理テーブル 231 から、ソフト ID を含むソフトウェア管理情報を読み出す。次に、判定部 214 は、読み出した部分ソフトウェア管理情報から前半ソフト署名データを抽出し、読み出したソフトウェア管理情報から後半ソフト署名データを抽出し、抽出

した前半ソフト署名データ及び抽出した後半ソフト署名データを結合してソフト署名データを生成する。

【0151】

以上説明したように、耐タンパモジュール部210は、さらに、情報記憶部218を備え、情報記憶部218は、ソフトウェア管理テーブルの一部を格納する。

具体的には、一例として、情報記憶部218は、ソフト署名データの少なくとも一部を格納する。第2記憶領域222が有するソフトウェア管理テーブル231は、ソフト署名データの残りの部分を格納する。判定部214は、情報記憶部218に含まれるソフト署名データの少なくとも一部と、第2記憶領域222から読み出したソフト管理情報に含まれるソフト署名データの残りの部分より、ソフト署名データ全体を復元して使用する。

【0152】

なお、ここでは、情報記憶部218にソフト署名データの前半部分を格納する構成について説明したが、この構成に限定されるものではない。

5. その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【0153】

(1) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0154】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0155】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(2) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0156】

【発明の効果】

以上説明したように、本発明は、ソフトウェアを記録している記録媒体と、前記ソフトウェアを内部に記録し、前記ソフトウェアに従って動作する情報処理装置とから構成される情報処理システムであって、前記記録媒体は、ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段とを備え、前記情報処理装置は、前記ソフトウェアを記憶するための領域を備える記憶手段と、前記記録媒体から前記許可指示を取得する取得手段と、取得した前記許可指示に応じて、前記記録媒体か

ら前記ソフトウェアを取得して前記記憶手段に書き込み、又は前記記憶手段に記憶されている前記ソフトウェアを非活性化する制御手段とを備える。また、ソフトウェアを記録している記録媒体であって、ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段とを備える。また、ソフトウェアを記録している記録媒体から、前記ソフトウェアを取得して内部に記録し、前記ソフトウェアに従って動作する情報処理装置であって、前記記録媒体は、ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断し、可と判断する場合に、前記情報処理装置に対してインストール又はアンインストールの許可を示す許可指示を出力し、インストール又はアンインストールに応じて前記セキュア記憶手段に記憶されているライセンス情報を書き換える耐タンパモジュール手段とを備え、前記情報処理装置は、前記ソフトウェアを記憶するための領域を備える記憶手段と、前記記録媒体から前記許可指示を取得する取得手段と、取得した前記許可指示に応じて、前記記録媒体から前記ソフトウェアを取得して前記記憶手段に書き込み、又は前記記憶手段に記憶されている前記ソフトウェアを非活性化する制御手段とを備える。

【0157】

これらの構成によると、外部から直接アクセスできないセキュア記憶手段にライセンス情報が記憶されているので、ライセンス情報の改竄が容易ではない。また、記録媒体から相手装置へライセンス情報が伝送されないので、記録媒体から

相手装置への通信路上においてライセンス情報が漏洩して改竄されることはない。さらに、ソフトウェアの使用条件に係るライセンス情報がセキュア記憶手段に記憶されているので、ライセンス情報とソフトウェアとの対応関係が不当に改竄されることはない。

【0158】

ここで、前記通常記憶手段は、ソフトキーを用いて暗号化された暗号化ソフトウェアを記憶しており、前記セキュア記憶手段は、前記ソフトキーを含む前記ライセンス情報を記憶しており、前記耐タンパモジュール手段は、インストール可と判断する場合に、前記セキュア記憶領域に記憶されているライセンス情報からソフトキーを抽出し、抽出したソフトキーをセキュアに出力する。

【0159】

この構成によると、暗号化ソフトウェアを暗号化するために用いられるソフトキーを、耐タンパモジュール手段がセキュアに出力するので、ソフトキーが不当に改竄されることがない。

ここで、前記セキュア記憶手段は、前記ソフトウェアの署名データを含む前記使用条件に係る前記ライセンス情報を記憶しており、前記耐タンパモジュール手段は、インストールを可と判断する場合に、さらに、前記セキュア記憶手段に記憶されているライセンス情報から前記署名データを抽出し、抽出した前記署名データを出力する。

【0160】

この構成によると、耐タンパモジュール手段がソフトウェアの署名データを出力するので、署名データが改竄されることはない。

ここで、前記セキュア記憶手段は、前記使用条件が所定のキー情報を用いて暗号化されて生成された前記ライセンス情報を記憶しており、前記耐タンパモジュール手段は、前記キー情報を記憶しており、前記キー情報を用いて、前記ライセンス情報を復号して前記使用条件を生成し、生成した使用条件に基づいて、前記情報処理装置を対象とするソフトウェアのインストール又はアンインストールの可否を判断する。

【0161】

この構成によると、前記セキュア記憶手段は、前記使用条件が所定のキー情報を用いて暗号化されて生成された前記ライセンス情報を記憶しており、前記耐タンパモジュール手段は、記憶している前記キー情報を用いて、前記ライセンス情報を復号して前記使用条件を生成するので、正当なキー情報を記憶している前記耐タンパモジュール手段のみが前記ライセンス情報を使用することができる。

【0162】

ここで、前記セキュア記憶手段は、前記ライセンス情報の一部分を記憶しており、前記耐タンパモジュール手段は、さらに、前記ソフトウェアの他の部分を記憶しており、インストール又はアンインストールを可と判断する場合に、さらに、前記セキュア記憶手段に記憶されているライセンス情報の前記一部分を抽出し、抽出した前記一部分と記憶している前記他の部分とからライセンス情報を生成する。

【0163】

この構成によると、前記セキュア記憶手段は、ライセンス情報の一部分を記憶しており、前記耐タンパモジュール手段は、前記ライセンス情報の他の部分を記憶しており、これらから全体のライセンス情報を生成するので、ライセンス情報が改竄される可能性をさらに低減することができる。

ここで、前記セキュア記憶手段が記憶しているライセンス情報は、前記ソフトウェアの使用許可回数であり、前記耐タンパモジュール手段は、前記使用許可回数が0より大きいと判断する場合に、前記ソフトウェアの使用が許可されたとみなして、前記許可指示、前記ソフトキー、もしくは前記署名データのうち、少なくとも一つを出力し、さらに、前記使用許可回数から1減じて前記セキュア記憶手段に書き込む。

【0164】

この構成によると、前記ライセンス情報は、前記ソフトウェアの使用許可回数であり、インストールの際に、前記耐タンパモジュール手段は、前記使用許可回数が0より大きいと判断する場合に、前記使用許可回数から1を減じて前記セキュア記憶手段に書き込むので、前記ソフトウェアの使用回数を確実に管理することになる。

【0165】

ここで、前記セキュア記憶手段が記憶しているライセンス情報は、前記ソフトウェアの使用許可回数であり、前記耐タンパモジュール手段は、前記ソフトウェアのアンインストールが許可された場合に、前記許可指示を出力し、さらに、前記使用許可回数を1加算して前記セキュア記憶手段に書き込む。

この構成によると、前記ライセンス情報は、前記ソフトウェアの使用許可回数であり、アンインストールの際に、前記使用許可回数に1を加算して前記セキュア記憶手段に書き込むので、前記ソフトウェアの使用回数を確実に管理することができる。

【0166】

また、本発明は、ソフトウェアを記録している記録媒体であって、ソフトウェアを記憶している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断し、許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出し、読み出した前記署名データを出力する耐タンパモジュール手段とを備える。

【0167】

この構成によると、外部から直接アクセスできないセキュア記憶手段にライセンス情報が記憶されているので、ライセンス情報の改竄が容易ではない。また、記録媒体から相手装置へライセンス情報が伝送されないので、記録媒体から相手装置への通信路上においてライセンス情報が漏洩して改竄されることはない。さらに、ライセンス情報とソフトウェアの署名データとがセキュア記憶手段に記憶されているので、ライセンス情報とソフトウェアとの対応関係が不当に改竄されることはない。

【0168】

また、ソフトウェアを記録している記録媒体から前記ソフトウェアを読み出して内部に記憶する情報処理装置であって、前記記録媒体は、ソフトウェアを記憶

している通常記憶手段と、前記ソフトウェアの署名データと、前記ソフトウェアの使用条件に係るライセンス情報を記憶しており、外部から直接アクセスできないセキュア記憶手段と、耐タンパ性を有し、前記セキュア記憶手段に記憶されているライセンス情報に基づいて、前記ソフトウェアの使用が許可されているか否かを判断し、許可されていると判断する場合に、前記セキュア記憶手段から署名データを読み出し、読み出した前記署名データを出力する耐タンパモジュール手段とを備え、前記情報処理装置は、前記記録媒体から前記署名データ及び前記ソフトウェアを取得する取得手段と、取得した前記署名データを用いて、取得した前記ソフトウェアの検証を行い、検証が成功した場合に、取得した前記ソフトウェアを内部に記憶する記憶手段とを備える。

【0169】

この構成によると、前記記録媒体から取得した前記署名データを用いて、取得した前記ソフトウェアの検証を行い、検証が成功した場合に、取得した前記ソフトウェアを内部に記憶するので、正当なソフトウェアのみを取得して内部に記憶することができる。

【図面の簡単な説明】

【図1】

ソフトウェア管理システム10の構成を示す。

【図2】

ソフトウェア書込装置100及びメモリカード200の構成を示すブロック図である。

【図3】

メモリカード200及び情報処理装置300の構成を示すブロック図である。

【図4】

ソフトウェア管理情報テーブル231のデータ構造の一例を示す。

【図5】

ソフトウェア管理システム10の動作を示すフローチャートである。特に、メモリカード200から情報処理装置300へソフトウェアがインストールされる場合、又はアンインストールされる場合の動作を示している。図6へ続く。

【図 6】

ソフトウェア管理システム 10 の動作を示すフローチャートである。特に、メモリカード 200 から情報処理装置 300 へソフトウェアがインストールされる場合、又はアンインストールされる場合の動作を示している。図 7 へ続く。

【図 7】

ソフトウェア管理システム 10 の動作を示すフローチャートである。特に、メモリカード 200 から情報処理装置 300 へソフトウェアがインストールされる場合、又はアンインストールされる場合の動作を示している。図 8 へ続く。

【図 8】

ソフトウェア管理システム 10 の動作を示すフローチャートである。特に、メモリカード 200 から情報処理装置 300 へソフトウェアがインストールされる場合、又はアンインストールされる場合の動作を示している。図 7 から続く。

【図 9】

判定部 214 における詳細の動作を示すフローチャートである。

【図 10】

変形例としてのソフトウェア管理システム 10b を構成するソフトウェア書込装置 100b 及びメモリカード 200b の構成を示すブロック図である。

【図 11】

ソフトウェア管理情報のデータ構造の一例を示す。

【図 12】

ソフトウェア管理システム 10b を構成するメモリカード 200b 及び情報処理装置 300b の構成を示すブロック図である。

【図 13】

別の変形例としてのソフトウェア管理システム 10c を構成するメモリカード 200c 及び情報処理装置 300c の構成を示すブロック図である。

【図 14】

別の変形例としてのソフトウェア管理システム 10d を構成するメモリカード 200d 及び情報処理装置 300d の構成を示すブロック図である。

【図 15】

部分ソフトウェア管理テーブル 2 1 9 及びソフトウェア管理情報テーブル 2 3
1 の一例としてのデータ構造を示す。

【符号の説明】

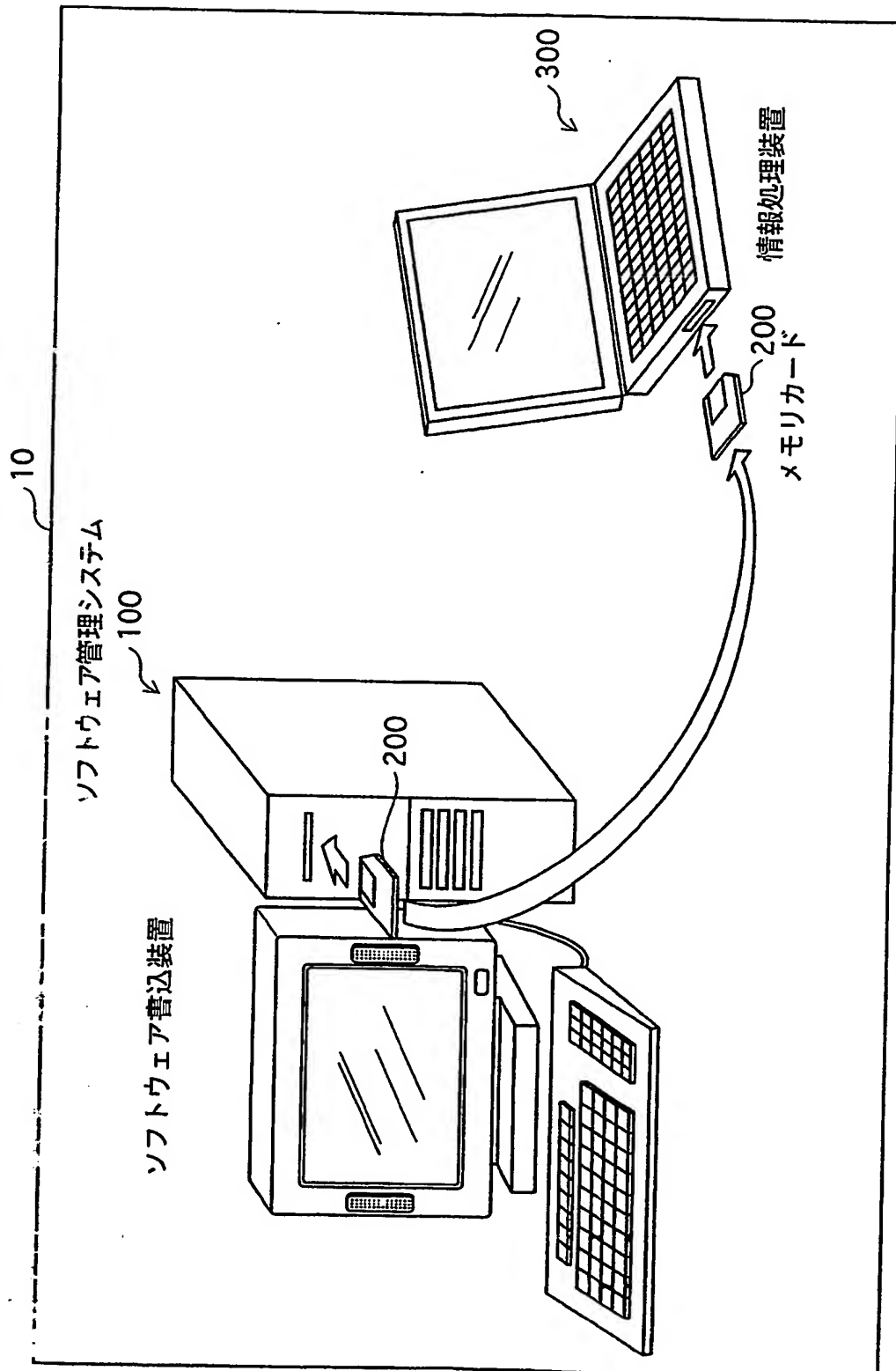
1 0	ソフトウェア管理システム
1 0 0	ソフトウェア書込装置
1 1 1	認証部
1 1 2	暗号化部
1 1 3	情報記憶部
1 1 4	制御部
1 1 5	入力部
1 1 6	表示部
1 1 7	署名生成部
1 1 8	入出力部
2 0 0	メモリカード
2 1 0	耐タンパモジュール部
2 1 1	認証部
2 1 2	復号部
2 1 3	暗号化部
2 1 4	判定部
2 1 5	復号部
2 1 6	暗号化部
2 1 7	キー情報記憶部
2 2 0	情報記憶部
3 0 0	情報処理装置
3 1 0	インストール処理部
3 1 1	認証部
3 1 2	暗号化部
3 1 3	復号部
3 1 4	復号部

- 3 1 5 暗号化部
- 3 1 6 装置 I D 格納部
- 3 1 7 装置固有鍵生成部
- 3 1 8 ソフト I D 取得部
- 3 1 9 署名検証部
- 3 2 0 ソフトウェア格納部
- 3 2 1 制御部
- 3 2 2 表示部
- 3 2 3 入力部
- 3 2 4 ソフトウェア実行部
- 3 2 5 復号部

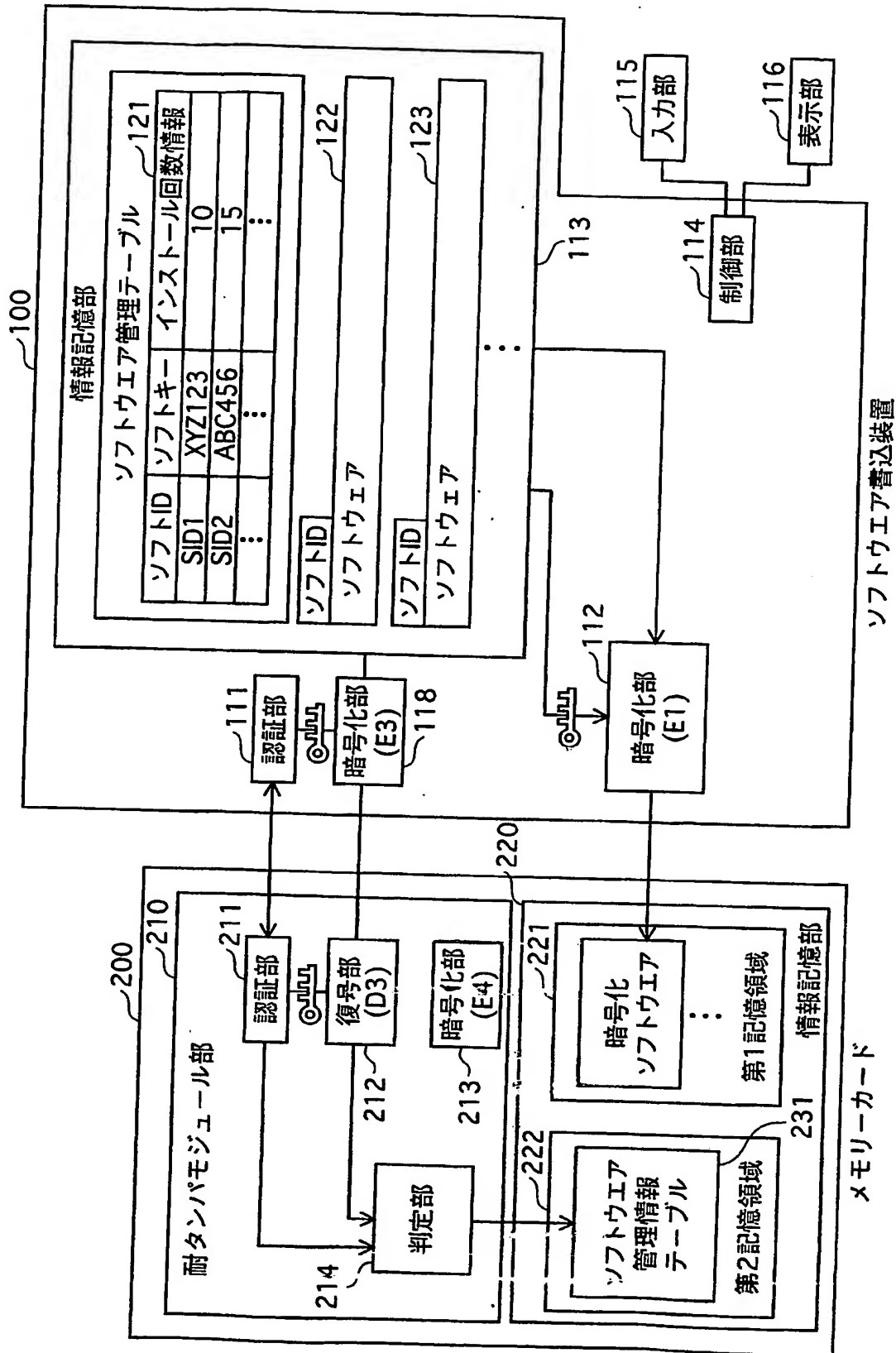
【書類名】

図面

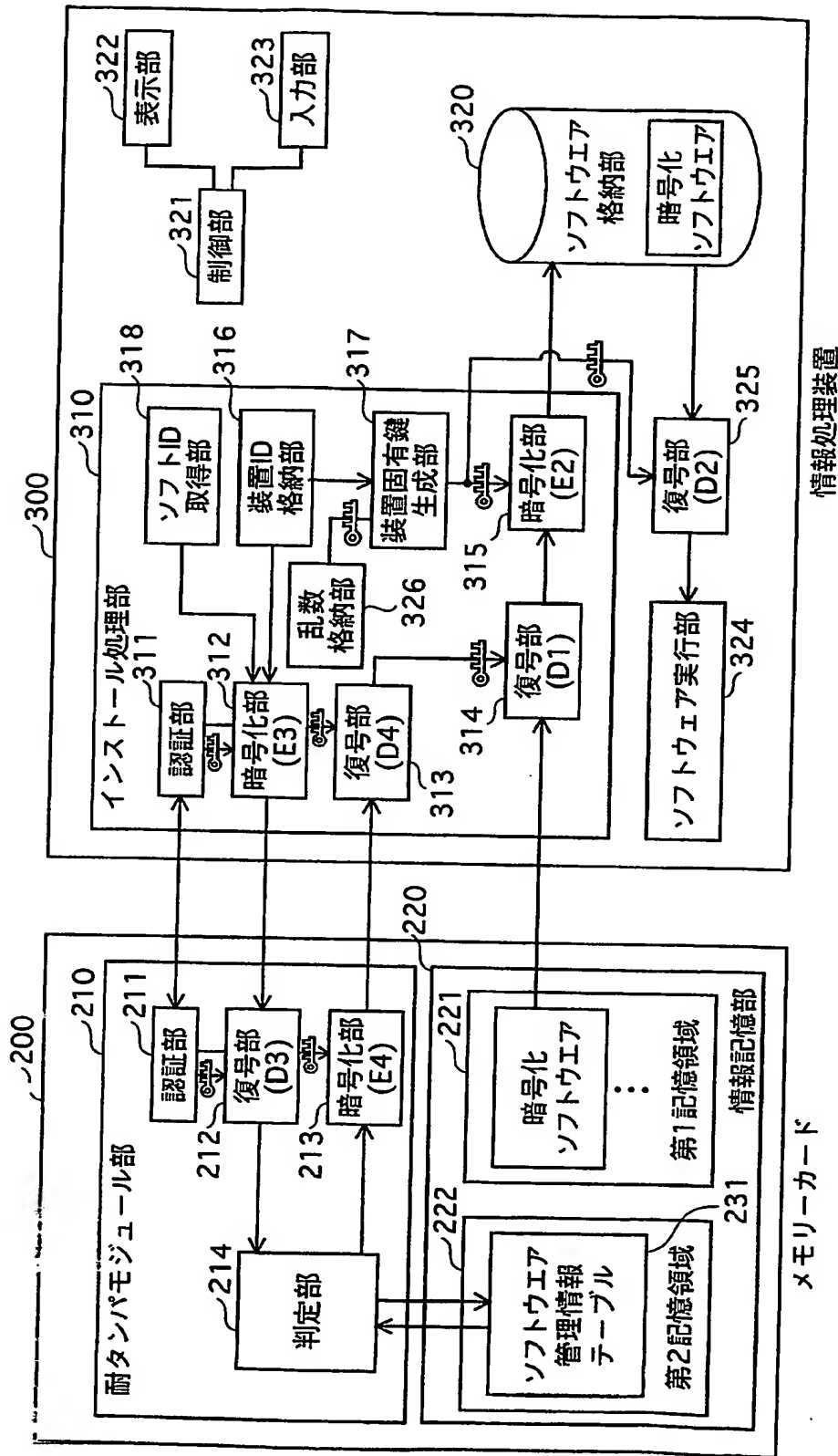
【図 1】



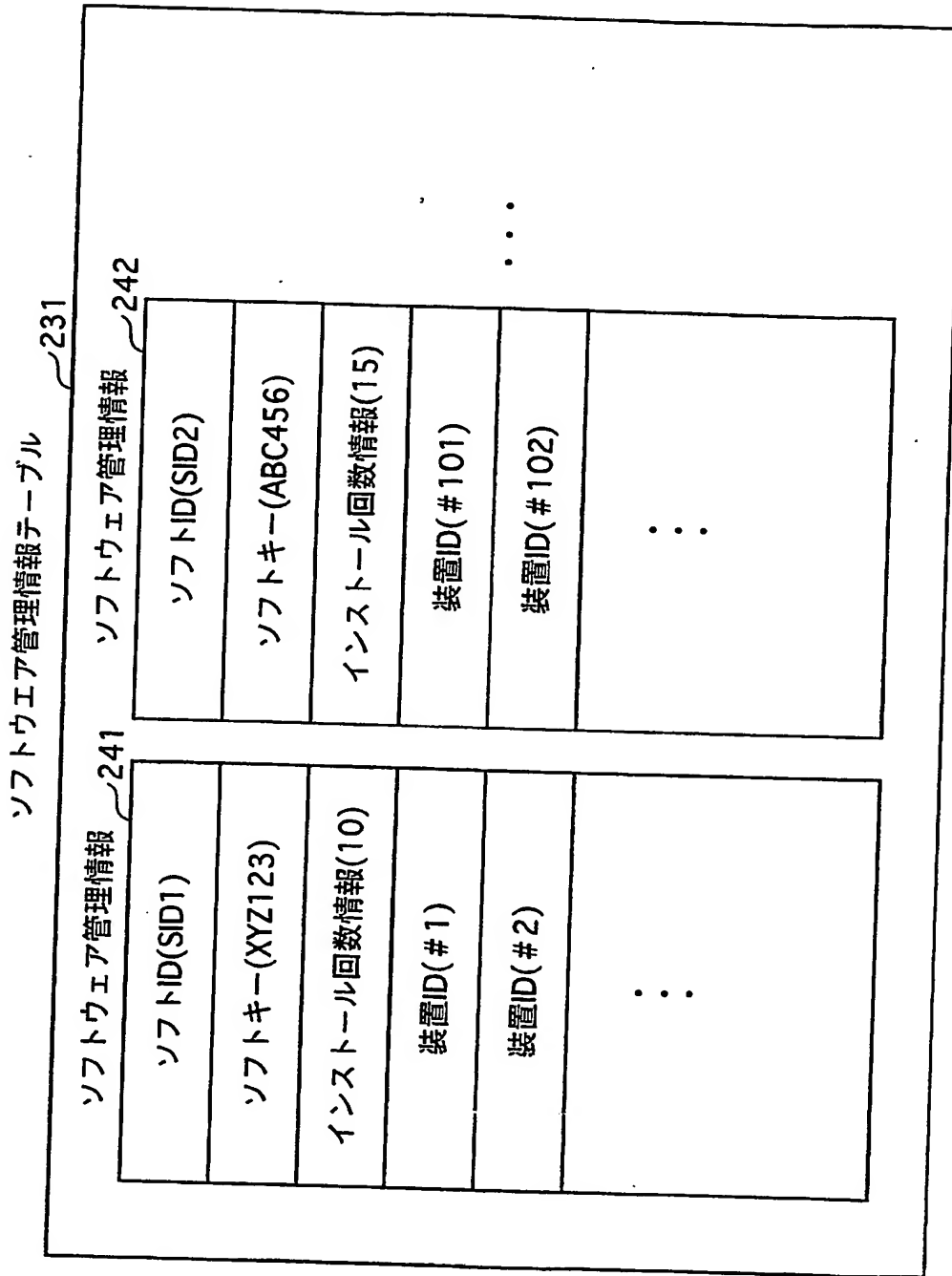
【図 2】



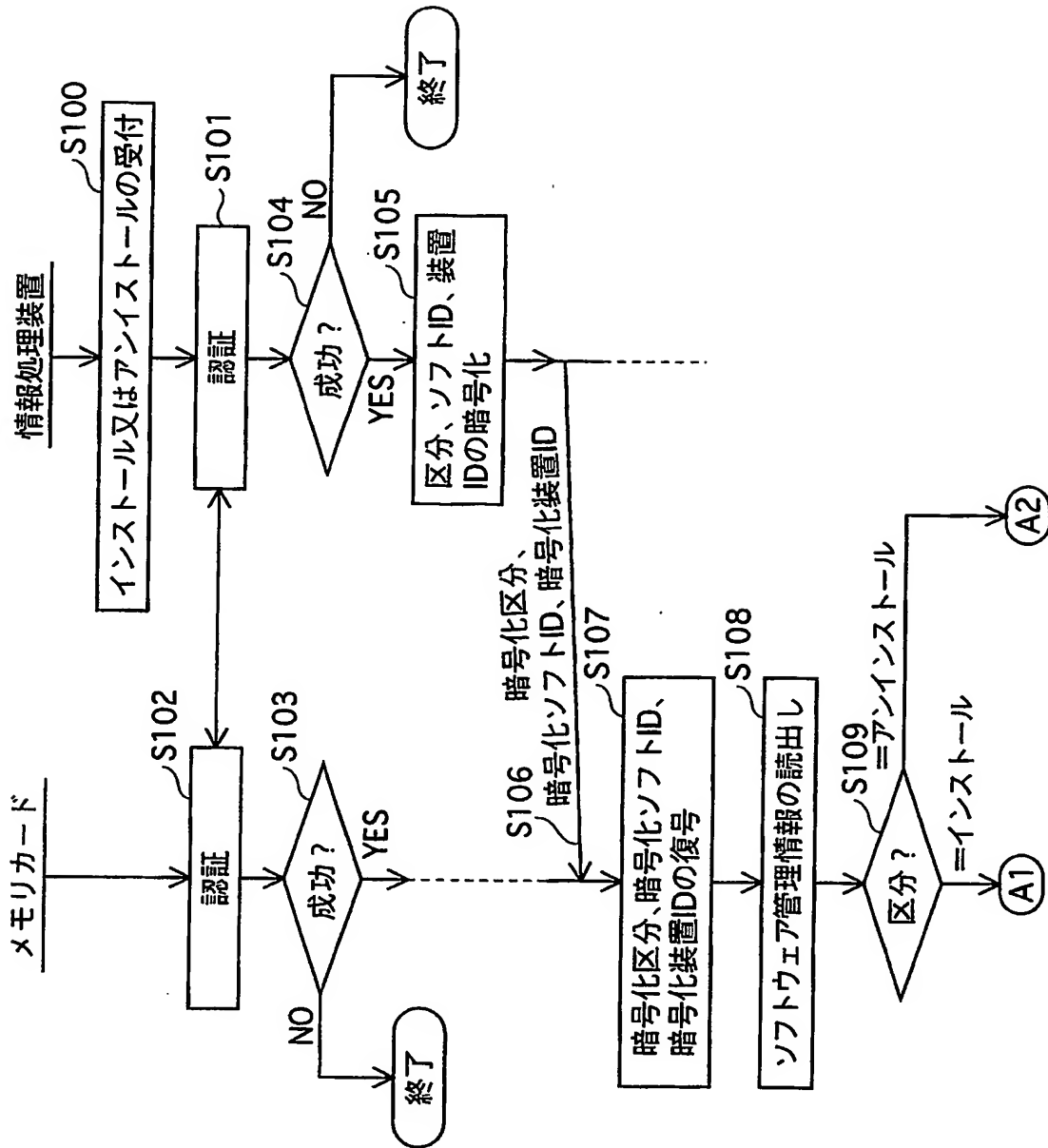
【図3】



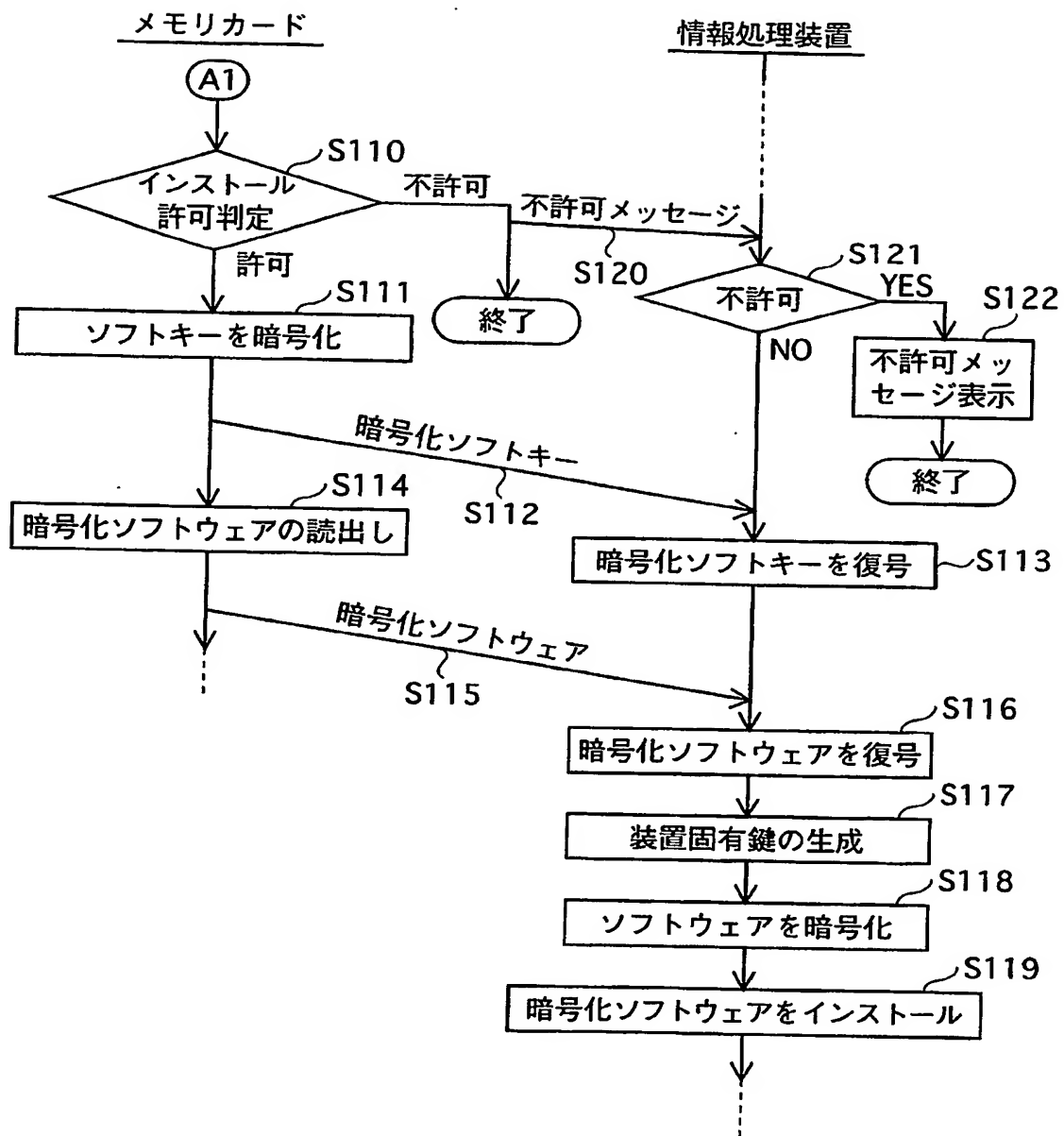
【図 4】



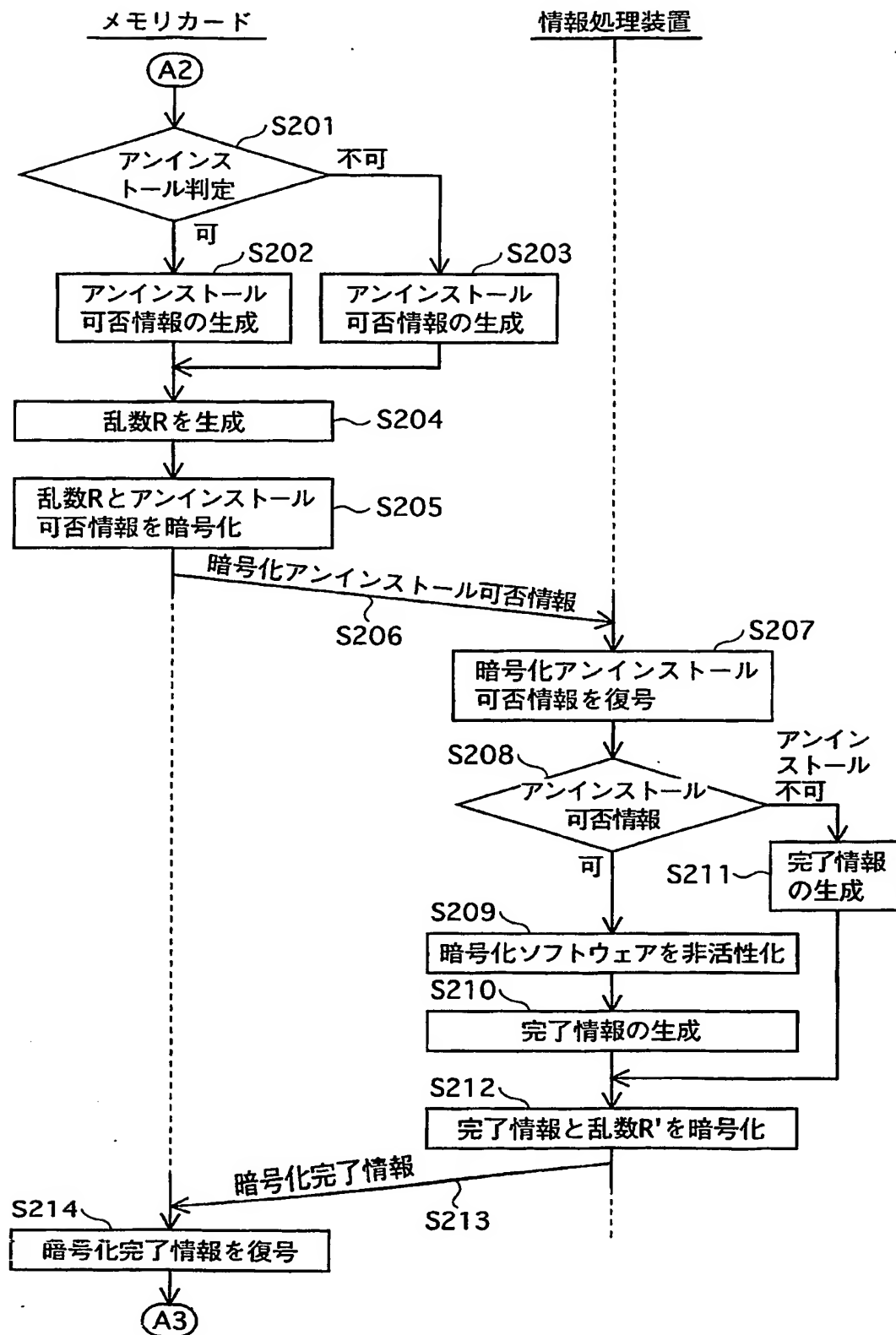
【図5】



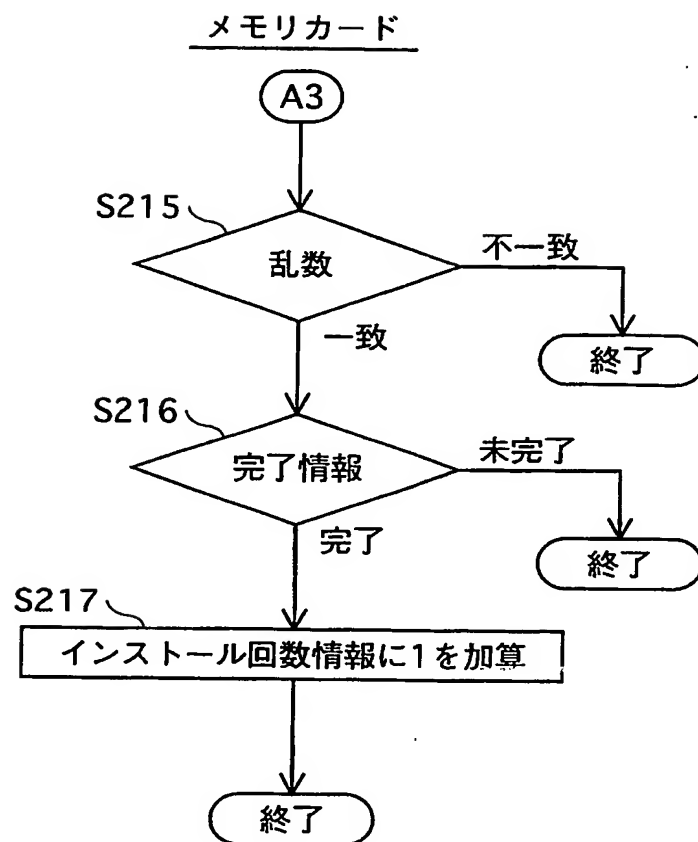
【図 6】



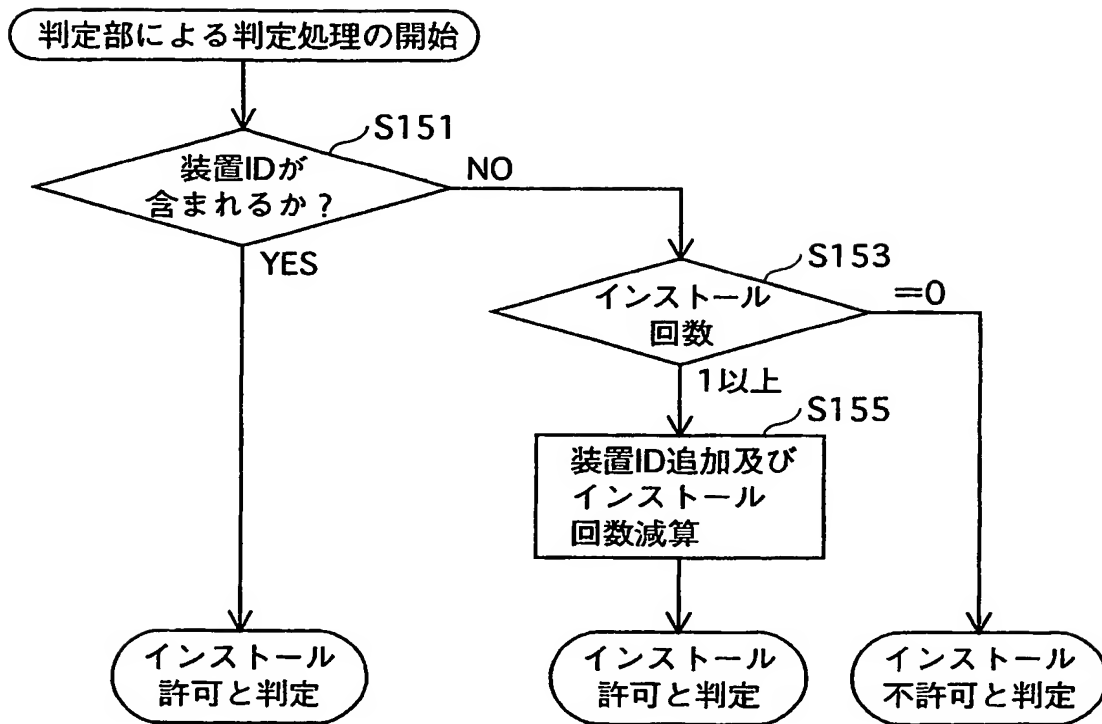
【図 7】



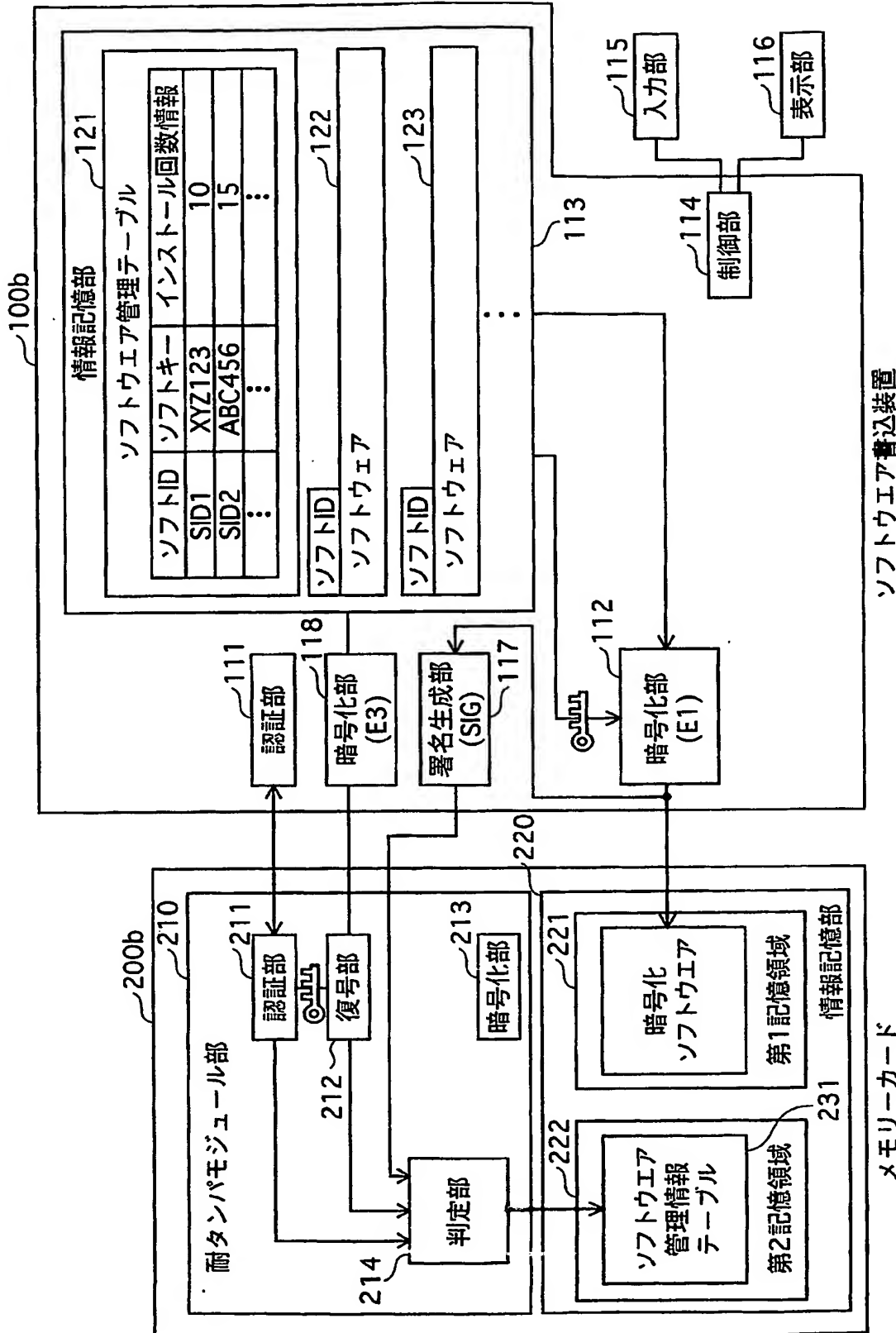
【図8】



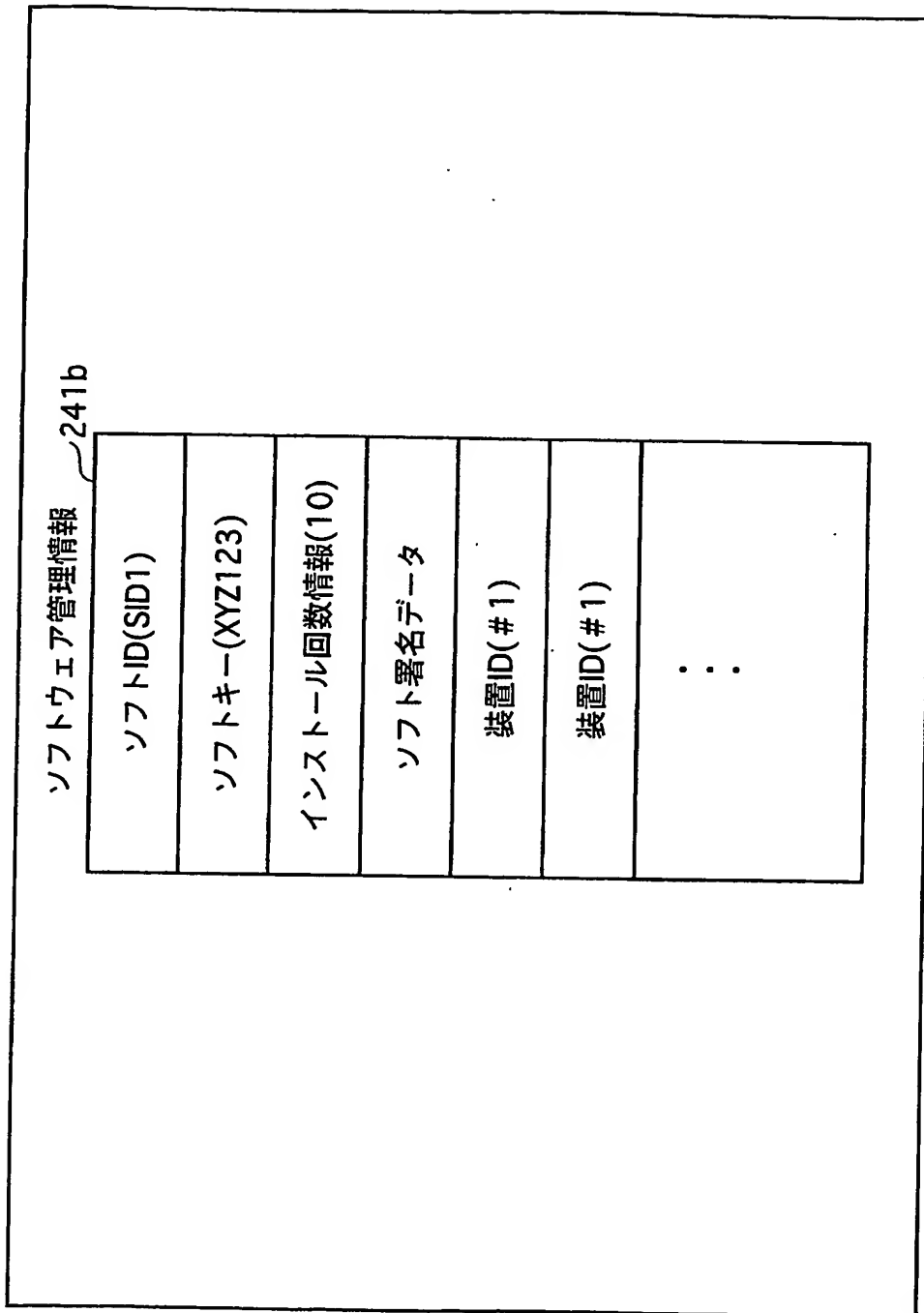
【図 9】



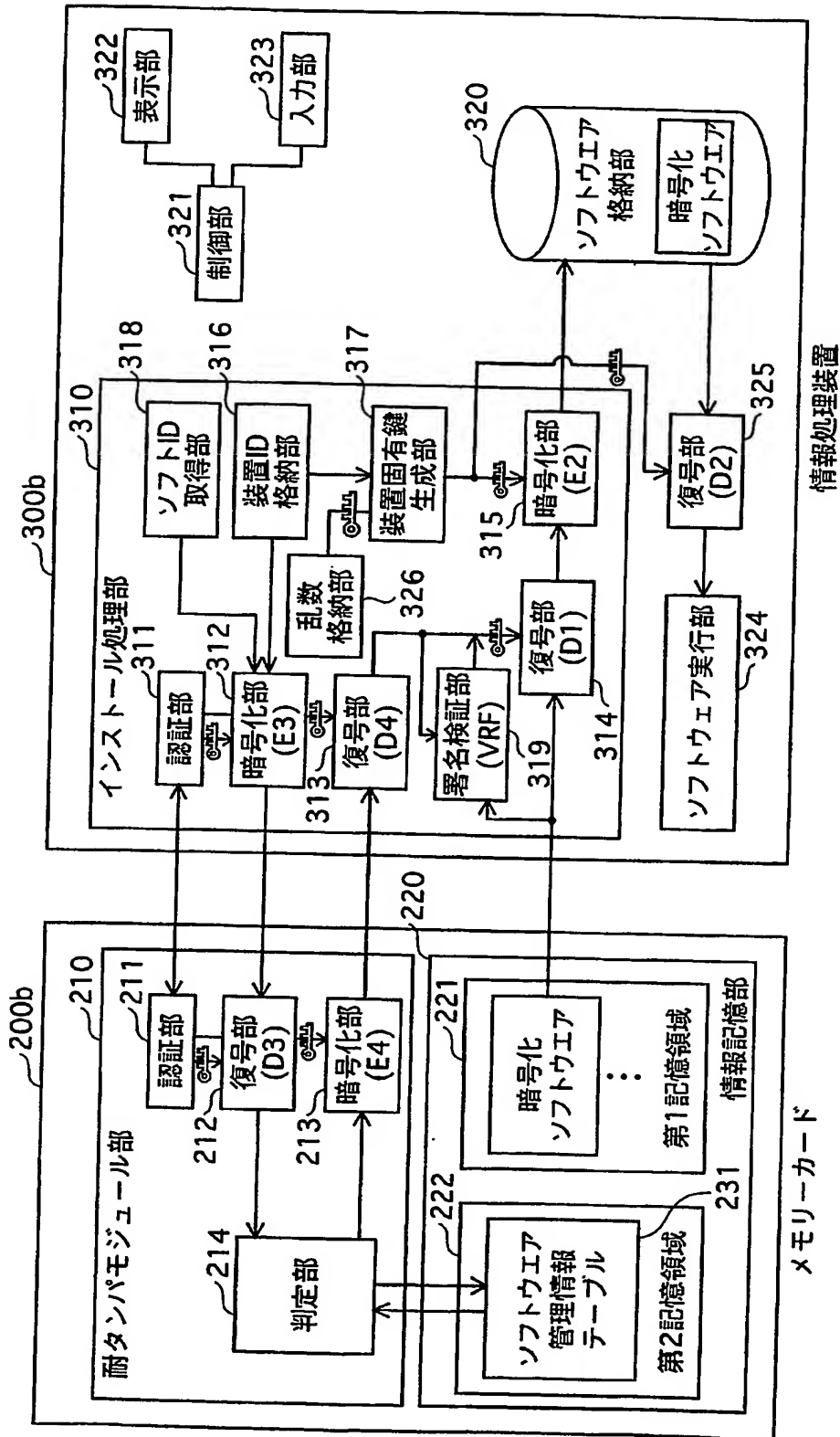
【図10】



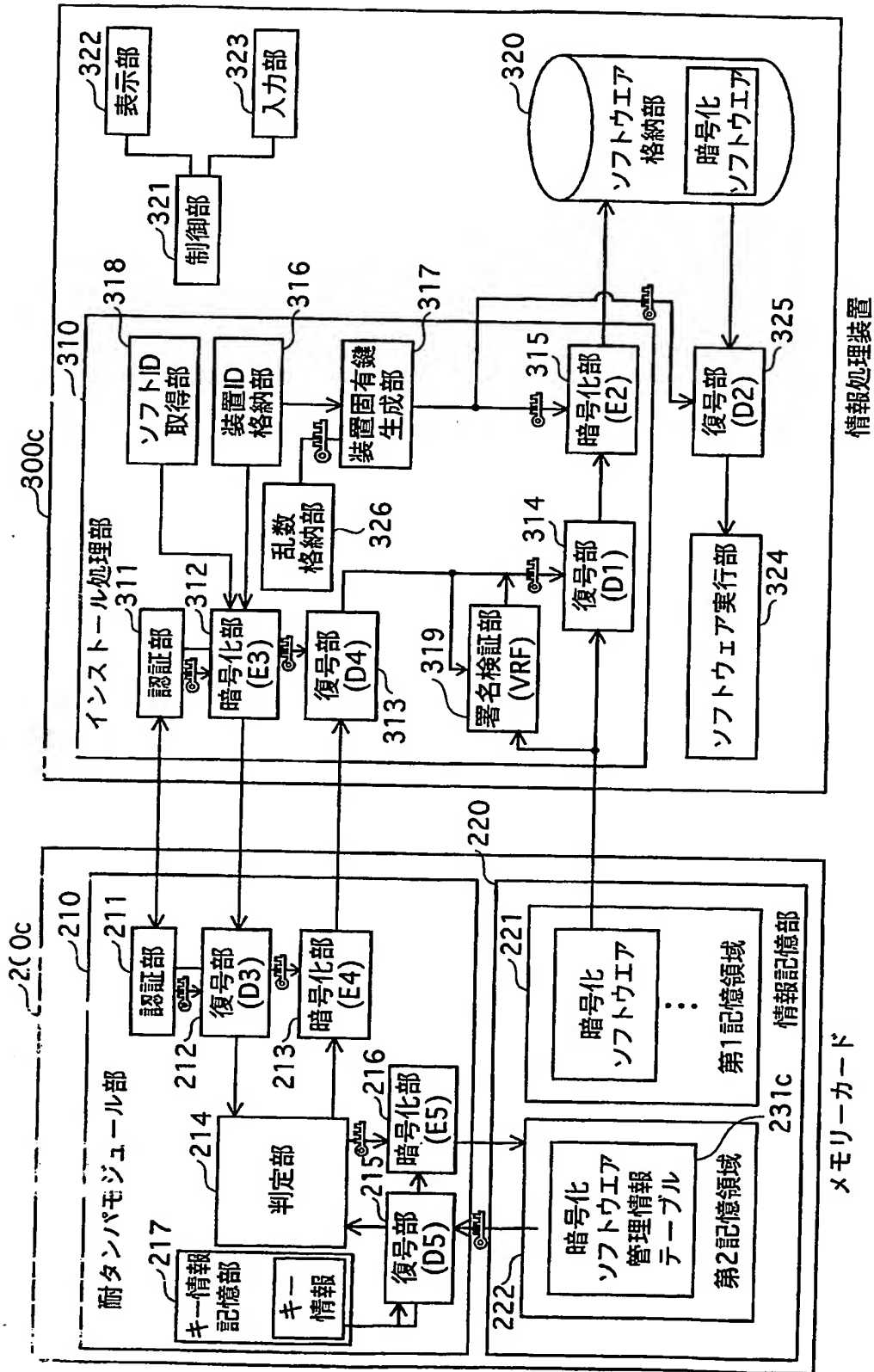
【図 11】



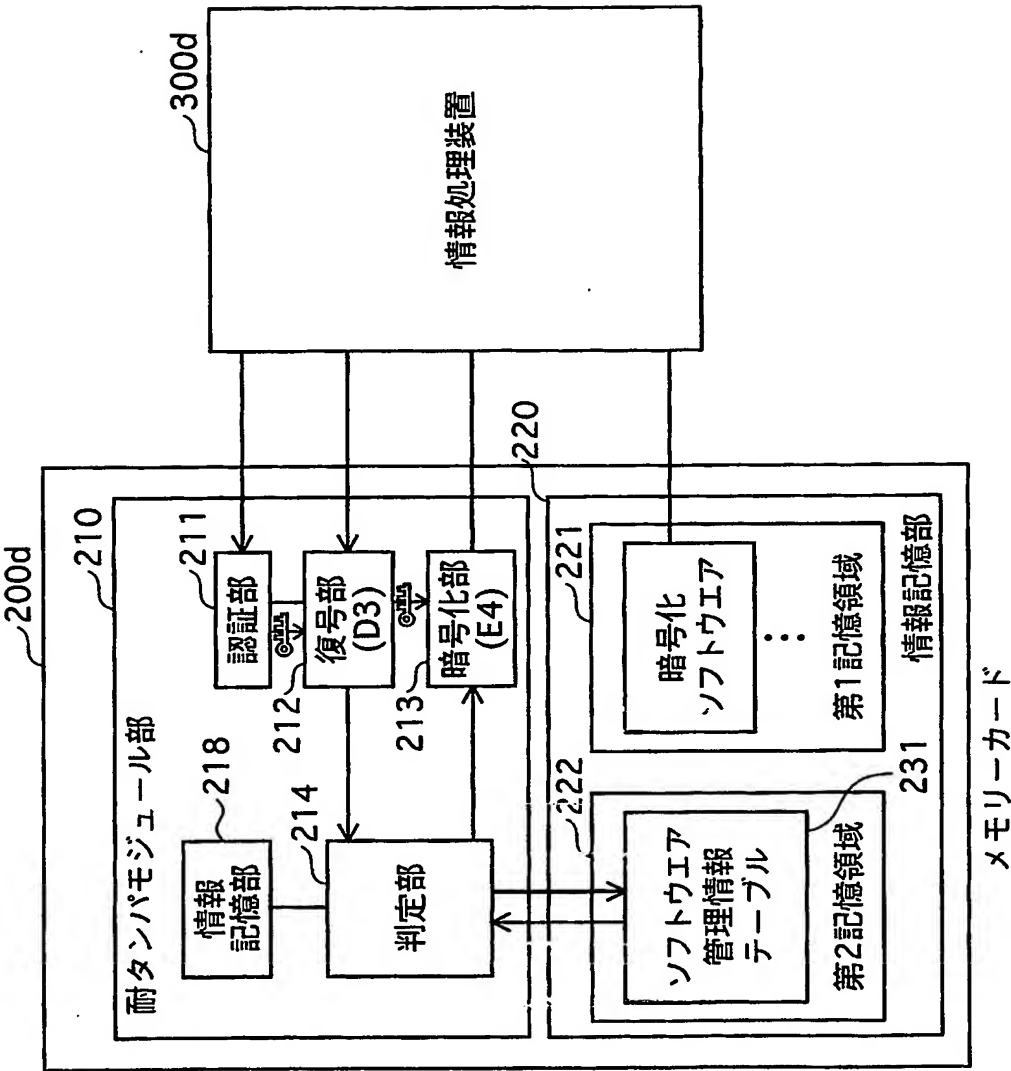
【図 12】



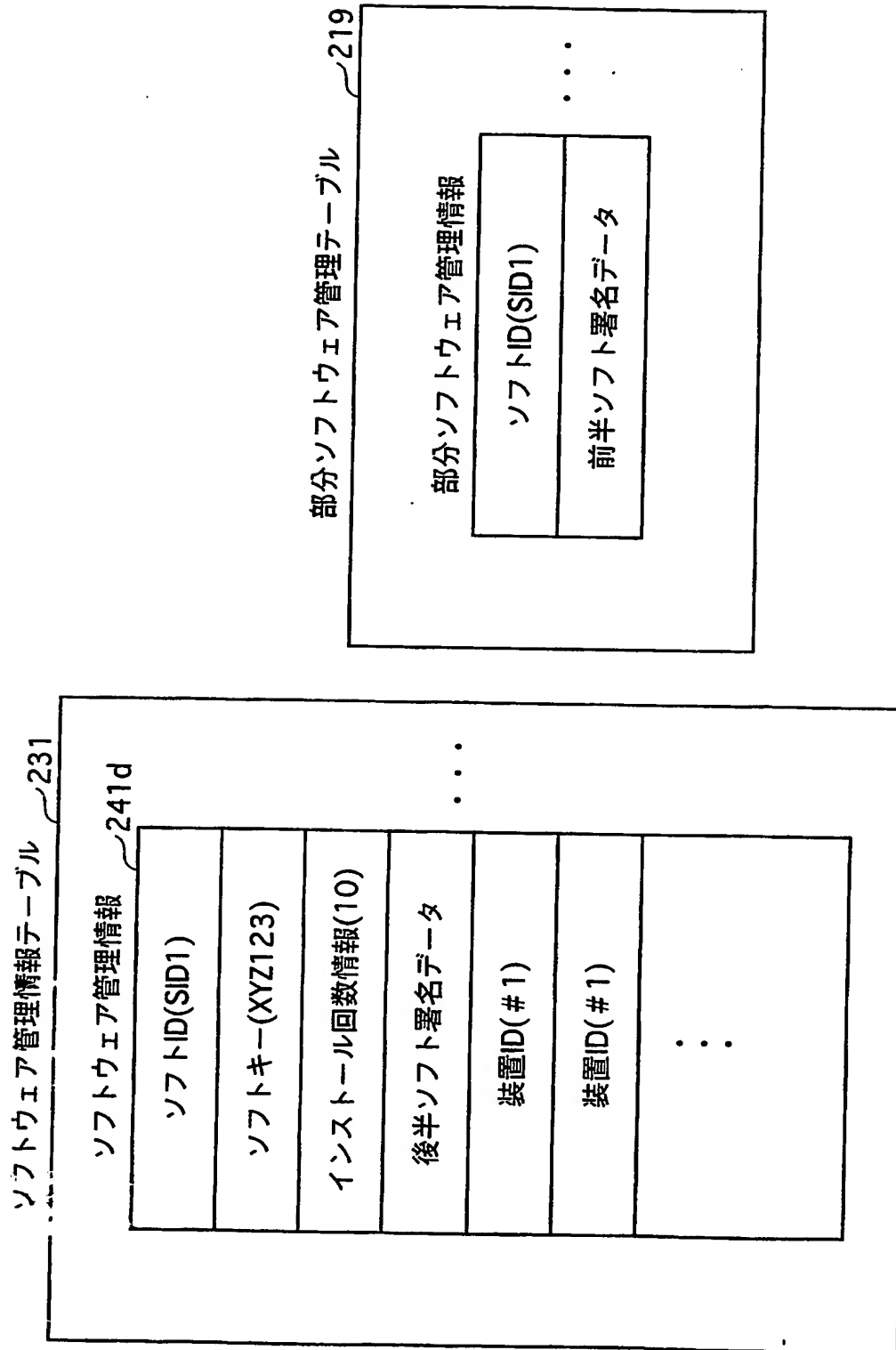
【図13】



【図14】



【図 15】



【書類名】 要約書

【要約】

【課題】 記録媒体上の改竄がされにくく、インストールの対象の端末装置と記録媒体との間の通信路における不当な攻撃を避けることができ、またソフトウェアとライセンス情報との対応関係を不正に更新することができない記録媒体を提供する。

【解決手段】 記録媒体は、セキュア記憶領域及び通常記憶領域を含む情報記憶部と、耐タンパモジュール部とを備えている。通常記憶領域には、ソフトウェアが、セキュア記憶領域には、前記ソフトウェアの使用許可数を示すライセンス数と、前記ソフトウェアの署名データとが対応付けて記録されている。耐タンパモジュール部は、端末装置との間で相互に機器認証を行い、セキュア記憶領域のライセンス数が所定数以内であれば、ソフトウェアと署名データとを端末装置へ出力する。

【選択図】 図3

特願 2 0 0 3 - 0 4 5 1 0 7

ページ : 1/E

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日
[変更理由]
住 所
氏 名

1 9 9 0 年 8 月 2 8 日
新規登録
大阪府門真市大字門真 1 0 0 6 番地
松下電器産業株式会社